



UNIVERSIDAD DE CONCEPCIÓN
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

GENERACIÓN PROBABILÍSTICA DE ESTADOS DE BELL

Por: David Antonio Montoya Sepúlveda

Tesis presentada a la Facultad de Ciencias Físicas y Matemáticas de la
Universidad de Concepción para optar al grado académico de Magíster en
Ciencias con Mención en Física

Julio 2021

Concepción, Chile

Profesor Guía: Dr. Luis Roa Oppliger

Profesora Co-Guía: Dra. Ariana Muñoz Espinoza

Comisión: Dr. Claudio Faúndez Araya

Comisión: Dr. Joaquín Díaz de Valdes Olavarrieta

*“To see a world in a grain of sand
and a heaven in a wild flower
hold infinity in the palm of your hand
and eternity in an hour...”¹*



William Blake (1757 - 1827)

¹*Para ver el mundo en un grano de arena y el cielo en una flor silvestre, sostén el infinito en la palma de tu mano y la eternidad en una hora.*

AGRADECIMIENTOS

Quisiera partir agradeciendo a mi familia, que sin ellos gran parte de lo que soy no lo sería y por consiguiente, probablemente no habría llegado hasta aquí. Quisiera agradecerles igualmente, que pese a las dificultades económicas me han ayudado a financiar parte del magíster, ya que por haber prolongado mi estadía en este la Beca de Extensión no lo cubría.

Continuaré estos agradecimientos mencionando al Dr. Luis Roa, que me aceptó como uno de sus estudiantes y que me ayudó (no solo académicamente) cada vez lo que necesité. No podría dejar de mencionar a la Dra. Ariana Muñoz, que sin sus sugerencias, consejos y ayuda todo este camino de postgrado habría sido más difícil de lo que ya fue. Y por supuesto, agradecido de toda la planta docente del Departamento de Física por la formación que me dieron, a las secretarias por toda la ayuda que me brindaron a pesar de estar haciendo trámites al filo del plazo máximo y a los auxiliares, por su buena onda y comprensión cada vez que les pedía que me abrieran la oficina porque se me quedaban las llaves adentro.

Agradezco a mis compañeros de generación, con los que entré y con los que terminé, por los momentos de diversión, conversación, ayuda y todo lo vivido en este sendero que me ha traído hasta aquí. Me gustaría mencionar en especial a Esteban Roa, por todas esas conversaciones y discusiones que tuvimos, que sin duda me ayudaron a generar una mejor comprensión de muchos aspectos de la física y la no-física, porque *al igual que un tensor es algo que transforma como tensor ¿qué es un poeta, sino alguien que escribe poesías?*. También mencionar a Jorge Gidi, por las conversaciones de oficina y toda la ayuda brindada durante estos años.

Finalmente, dedico este párrafo de agradecimientos exclusivamente a Joselyn Rojas, mi pareja y compañera, por todo su cariño, comprensión y ayuda en todo este proceso de tesis y no-tesis. Por haberme enseñado y apoyado en todo aquello que tiene que ver con una tesis que no se ve plasmado en una tesis. Sin lugar a dudas, todo habría sido más difícil sin su colaboración y compañía.

Resumen

Se proponen dos estrategias que permiten obtener un estado maximalmente entrelazado (estado de Bell) a partir de un estado tripartito puro arbitrario, esto mediante una medición local adecuada. La primera estrategia consiste en utilizar el proceso de Extracción de Entrelazamiento Determinista seguido de un óptimo Método Procusteano. En la segunda estrategia, se realiza una medición local adecuada con el objetivo de optimizar la probabilidad total de éxito. Se encuentran soluciones analíticas para estas probabilidades máximas de éxito de lograr un estado de Bell. Finalmente, se analizan algunos casos particulares.



Keywords – Bell States, Threetangle, Concurrence, Entanglement, Deterministic Entanglement, Procrustean Method

Abstract

We propose two strategies, both allow to obtain a maximally entangled state from an arbitrary tripartite pure state by means of suitable local measurement. The first strategy consist of Deterministic Entanglement Extraction process followed by an optimal Procrustean Method. In the second strategy, a suitable local measurement is performed with the aim of optimizing the total success probability. We found analytical solutions for these maximal total success probabilities of achieving a maximally entangled state. Finally, we analyze some particular cases.



Keywords – Bell States, Threetangle, Concurrence, Entanglement, Deterministic Entanglement, Procrustean Method

Índice general

AGRADECIMIENTOS	I
Resumen	II
Abstract	III
1. Introducción	1
2. Probabilidad	3
2.1. Conceptos básicos	4
2.1.1. Evento aleatorio	4
2.1.2. Conjuntos	4
2.1.3. Operaciones de conjuntos	5
2.1.4. Álgebra de conjuntos	6
2.1.5. Espacio Muestral y Eventos	7
2.2. Definición clásica	7
2.3. Definición de frecuencia relativa	8
2.4. Definición axiomática	9
2.5. Probabilidades Condicionales y Marginales	11
3. Mecánica Cuántica	15
3.1. Espacio de Hilbert	16
3.2. Operadores Lineales y Matrices	17
3.2.1. Operadores adjuntos y hermíticos	19
3.2.2. Operadores Unitarios	20
3.2.3. Operadores de Pauli	21
3.2.3.1. Representación matricial	22
3.3. Postulados de la Mecánica Cuántica	23
3.3.0.1. Postulado 1: Estados	24
3.3.0.2. Postulado 2: Dinámica	24
3.3.0.3. Postulado 3: Observables	24
3.3.0.4. Postulado 4: Mediciones	25
3.3.0.5. Postulado 5: Composición	25
3.4. Operador Densidad	25
3.5. Reformulación de los Postulados	27

3.5.0.1.	Postulado 1: Estados	27
3.5.0.2.	Postulado 2: Dinámica	27
3.5.0.3.	Postulado 3: Mediciones	27
3.5.0.4.	Postulado 4: Composición	28
4.	Teoría de la Información Cuántica	29
4.1.	Qubit	29
4.1.1.	Multiples qubits	31
4.2.	Entropía de von Neumann	32
4.3.	Entrelazamiento	34
4.3.1.	Revisión del concepto	34
4.3.2.	Definición	36
4.4.	Operaciones Cuánticas	37
4.4.1.	Operaciones Locales	38
4.4.2.	Operaciones Locales y Comunicación Clásica (LOCC)	40
4.5.	Cuantificación del entrelazamiento	41
4.5.1.	Entropía de Entrelazamiento	41
4.5.2.	Criterios para una medida de entrelazamiento	42
4.5.3.	Medidas de entrelazamiento para estados mixtos	42
4.5.4.	Entrelazamiento de Formación	43
4.5.5.	Entrelazamiento Residual o <i>Three-tangle</i>	44
4.6.	Clasificación de estados cuánticos	45
4.6.1.	Estado producto	45
4.6.2.	Estados separables	46
4.6.3.	Estado clásico	46
4.6.4.	Estados entrelazados	47
4.6.4.1.	Estados de Bell	47
4.6.4.2.	Estados W	47
4.6.4.3.	Estados Greenberger-Horne-Zeilinger (GHZ)	47
4.7.	Extracción de Entrelazamiento Determinista (DEE)	48
4.7.1.	Concurrencia, <i>three-tangle</i> y probabilidad	49
4.8.	Método Procusteano	50
5.	Generación probabilística de estados de Bell	52
5.1.	Probabilidad de éxito Método Procusteano	52
5.2.	Desarrollo de Estrategias	53
5.3.	Estrategia 1	53
5.4.	Estrategia 2	54
5.4.0.1.	Caso 1.	61
5.4.0.2.	Caso 2.	61
5.4.0.3.	Caso 3.	61
5.4.0.4.	Caso 4.	62
5.4.1.	Máxima probabilidad de éxito Estrategia 2	63
5.5.	Comparación	64
5.5.1.	Estrategia 1	64
5.5.2.	Estrategia 2	65

5.5.2.1. Comparación numérica y comparación entre estrategias	65
5.5.3. Estado Tripartito Inicial	65
5.5.4. Caso $\alpha = 1$ y $\beta = 0$	66
5.5.5. Caso $\alpha = 1/2$ y $\beta = 1/2$	71
5.5.6. Caso $\alpha = -1/\sqrt{6}$ y $\beta = -1/\sqrt{2}$	75
6. Conclusión	79
Bibliografía	81
Apéndices	85
A. Desigualdades de Bell y CHSH	85
B. Esquema de Extracción de Entrelazamiento Determinista	88
C. Método de multiplicadores de Lagrange	91



Índice de cuadros

2.5.1.La distribución de pelotas de acuerdo a tamaño y color.	12
2.5.2.La distribución de probabilidades de acuerdo a tamaño y color. . .	12



Índice de figuras

4.1.1.Representación de Esfera de Bloch de un qubit. <i>Fuente: Elaborado por el autor.</i>	30
5.5.1.[$\alpha = 1, \beta = 0$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. Secuencial (S) : Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. Solución numérica (SN) : Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Solución Analítica (SA) : Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Comparación : Probabilidad de éxito estrategia 2 obtenida de distintos modos. <i>Fuente: Elaborado por el autor.</i>	69
5.5.2.[$\alpha = 1, \beta = 0$] Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde). <i>Fuente: Elaborado por el autor.</i>	70
5.5.3.[$\alpha = 1/2, \beta = 1/2$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. Secuencial (S) : Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. Solución numérica (SN) : Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Solución Analítica (SA) : Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Comparación : Probabilidad de éxito estrategia 2 obtenida de distintos modos. <i>Fuente: Elaborado por el autor.</i>	73
5.5.4.[$\alpha = 1/2, \beta = 1/2$] Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde). <i>Fuente: Elaborado por el autor.</i>	74

5.5.5.[$\alpha = -1/\sqrt{6}, \beta = -1/\sqrt{2}$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. Secuencial (S) : Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. Solución numérica (SN) : Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Solución Analítica (SA) : Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). Comparación : Probabilidad de éxito estrategia 2 obtenida de distintos modos. <i>Fuente: Elaborado por el autor.</i>	77
5.5.6.[$\alpha = -1/\sqrt{6}, \beta = -1/\sqrt{2}$] Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde). <i>Fuente: Elaborado por el autor.</i>	78



Capítulo 1

Introducción

El entrelazamiento es una correlación puramente cuántica esencial en procesos de información cuántica, tales como codificación superdensa [20], teleportación de estados cuánticos [21], intercambio de entrelazamiento [22], criptografía cuántica [23], entre otros.

Los estados de Bell son estados bipartitos maximalmente entrelazados [5] y juegan un rol importante en los procesos anteriormente mencionados. Dado esto, resulta relevante tener métodos para generarlos.

En un artículo publicado el 2019, fue introducido el concepto de *Entrelazamiento Determinista*. En dicho artículo, se presenta el esquema de Extracción de Entrelazamiento Determinista [46], el cual permite transferir correlaciones cuánticas presentes en un estado con la ayuda de un proceso de medición local adecuado. Las correlaciones cuánticas involucradas son la concurrencia [42] del par de qubits no medido y el *three-tangle* [45], ambas contenidas en un estado puro de un sistema de qubits tripartito. Este esquema garantiza que cualquiera sea el resultado de una medición local, ambos estados bipartitos resultantes son puros y tienen la misma cantidad de entrelazamiento. Cuando el proceso es óptimo, la cantidad de entrelazamiento determinista extraída es máxima [46].

Por otro lado, el Método Procusteano [36] permite transformar, probabilísticamente, un estado puro parcialmente entrelazado a un estado maximalmente entrelazado. Este método se vuelve óptimo cuando la probabilidad es máxima [36]. En este caso, si el proceso no es exitoso, el estado resultante

carece de entrelazamiento.

La presente tesis tiene por objetivo desarrollar y comparar dos estrategias probabilísticas para generar estados de Bell a partir de un estado tripartito puro.

Teniendo en mente lo anterior surge la siguiente pregunta, dado un estado tripartito puro $|\psi\rangle$, ¿cuál de las dos estrategias provee la mayor probabilidad de obtener un estado maximalmente entrelazado? En otras palabras, ¿cuál de los dos procesos a proponer es más probable de resultar en un estado de Bell?

Para desarrollar la primera estrategia, se considerarán los dos estados resultantes de la Extracción de Entrelazamiento Determinista óptima y luego se aplicará un óptimo Método Procusteano para alcanzar probabilísticamente un estado de maximalmente entrelazado. Se encontrará una expresión para la probabilidad total de éxito de esta estrategia.

En el desarrollo de la segunda estrategia, se optimizará el proceso de medición local con el propósito de proyectar los dos qubits no medidos a un estado maximalmente entrelazado. Cuando el proceso no es exitoso, los dos qubits no medidos son transferidos a un estado puro parcialmente entrelazado. Para este caso, se aplicará un óptimo Método Procusteano para llevar dicho estado a un estado maximalmente entrelazado. Así, en esta estrategia hay dos oportunidades para alcanzar un estado de Bell, y se encontrará una expresión analítica para la probabilidad total de éxito.

El presente trabajo se estructura de la siguiente manera: En el capítulo 2 se presentan nociones y definiciones asociadas al tema de probabilidad. En el capítulo 3 se desarrollan las nociones de álgebra lineal necesarias para entender los postulados de la mecánica cuántica, además de presentarse dichos postulados. En el capítulo 4 se introducen los conceptos de qubit y entrelazamiento. Además, algunas de las formas existentes para cuantificar el entrelazamiento, el esquema de Extracción Determinista de Entrelazamiento y el Método Procusteano. En el capítulo 5 se desarrollan las estrategias para generar estados de Bell. Y finalmente el capítulo 6 contiene las conclusiones de este trabajo.

Capítulo 2

Probabilidad

La probabilidad es extremadamente útil en una amplia variedad de campos, específicamente en mecánica cuántica (dada su interpretación probabilística), teoría de la información y teoría de la información cuántica.

Si bien la noción de probabilidad y cómo interpretarla es en realidad una cuestión filosófica bastante delicada y su discusión escapa de los objetivos de este trabajo, es importante señalar que existen diferentes escuelas de pensamiento al respecto, y quizá la *frecuentista* y la *Bayesiana* sean las principales.

La visión *frecuentista* interpreta a la probabilidad como una frecuencia a largo plazo en un gran número de repeticiones de un experimento: si decimos que una moneda tiene una probabilidad de $1/2$ de salir cara, esto significa que si lanzamos la moneda una y otra y otra ... y otra vez, esta caerá cara el 50% del tiempo.

La visión *Bayesiana* interpreta a la probabilidad como un grado de creencia acerca del evento en cuestión, por lo que podemos asignar probabilidades a hipótesis como “el candidato A ganará las elecciones” o “el acusado es culpable”, incluso si no es posible repetir la misma elección o el mismo crimen una y otra vez.

En lugar de profundizar en cuestiones filosóficas sobre la idoneidad del razonamiento probabilístico, simplemente daremos por sentado que la teoría de la probabilidad es útil en una amplia variedad de contextos, y a lo largo de esta tesis adoptaremos una interpretación frecuentista.

Este capítulo está basado principalmente en [1] y toma elementos de [2, 3].

2.1. Conceptos básicos

2.1.1. Evento aleatorio

Cualquier suceso o experimento cuyo resultado es incierto o, si es prácticamente imposible de predecir a partir de su estado inicial, se llama *evento aleatorio*. Ejemplos de esto son: lanzar una moneda, sacar una carta de un mazo, tirar un dado, entre otros; siempre y cuando la moneda, el mazo de cartas y el dado no estén arreglados.

2.1.2. Conjuntos

Un *conjunto* es una colección de objetos llamados *elementos*, los que no necesariamente tienen alguna estructura adicional o propiedades.

La entidad más fundamental en cualquier rama de las matemáticas es la de un *conjunto universal*, que es la colección de todos los objetos bajo consideración. Por ejemplo, el conjunto universal de la geometría plana es una superficie plana y el de la geometría espacial es el espacio tridimensional. El conjunto universal del cálculo, es el conjunto de los números reales (o la recta real) y el plano complejo es el conjunto universal del análisis complejo. El conjunto universal genérico se denota por \mathcal{S} , pero cada conjunto universal específico tiene su propio símbolo: \mathbb{R} es el conjunto de los números reales, \mathbb{C} es el conjunto de los números complejos, \mathbb{Z} es el conjunto de los números entero y \mathbb{N} es el conjunto de los números naturales.

Se escribe $a \in A$ para expresar el hecho de que a es un elemento de A y $a \notin A$ para denotar que a no pertenece a A . Además, un conjunto puede no tener elementos, en cuyo caso es llamado conjunto vacío y se simboliza por \emptyset .

Los conjuntos pueden ser especificados de una variedad de formas. Si \mathcal{S} contiene un número finito de elementos, x_1, x_2, \dots, x_n , se escribe como una lista de elementos encerrados entre paréntesis de llave:

$$\mathcal{S} = \{x_1, x_2, \dots, x_n\}.$$

Si \mathcal{S} contiene infinitos elementos x_1, x_2, \dots, x_n , los cuales pueden ser enumerados

en una lista¹ se escribe:

$$\mathcal{S} = \{x_1, x_2, \dots\}.$$

Alternativamente, se puede considerar el conjunto de todos los x que tienen cierta propiedad \mathcal{P} y se denota por

$$\{x|x \text{ satisface } \mathcal{P}\}.$$

Si cada elemento de un conjunto A es también un elemento de un conjunto B , se dice que A es un *subconjunto* de B y se denota por $A \subset B$. En particular, siempre se cumple que $\emptyset \subset A$, cualquiera sea el conjunto A . Además, si $A \subset B$ y $B \subset A$, entonces los dos conjuntos son *iguales* y se denota por $A = B$.

2.1.3. Operaciones de conjuntos

Dado dos conjuntos A y B se puede formar otro conjunto, llamado la *unión* de A y B y denotado por $A \cup B$, que consiste de todos los elementos pertenecientes a A o B o ambas:

$$A \cup B = \{x|x \in A \text{ o } x \in B\}.$$

La *intersección* de A y B , denotada por $A \cap B$, consiste de todos los elementos pertenecientes a A y B :

$$A \cap B = \{x|x \in A \text{ y } x \in B\}.$$

El *complemento* de un conjunto A , es el subconjunto del conjunto universal \mathcal{S} que contiene todos los elementos de \mathcal{S} que no están en A . Denotando este conjunto por A^c , se tiene

$$A^c = \{x|x \notin A\}.$$

Cuando $A \cap B = \emptyset$, se dice que A y B son *disjuntos*.

¹Es decir, hay tantos elementos como números enteros positivos

Una colección de conjuntos se llama una *partición* de un conjunto A si los conjuntos en la colección son disjuntos y su unión A .

2.1.4. Álgebra de conjuntos

Las operaciones de conjuntos tienen muchas propiedades que son consecuencias elementales de las definiciones. Algunos ejemplos son

$$\begin{aligned} A \cup B &= B \cup A, & A \cup (B \cup C) &= (A \cup B) \cup C, \\ (A^c)^c &= A, & A \cap A^c &= \emptyset, \\ A \cup \mathcal{S} &= \mathcal{S}, & A \cap \mathcal{S} &= A, \\ A \cup A^c &= \mathcal{S}, & A \cup \emptyset &= A. \end{aligned}$$

Se puede tomar la unión e intersección de una serie de conjuntos sin preocuparse por el orden de los conjuntos o dónde colocar los paréntesis, ya que estas operaciones son conmutativas y asociativas. Esto hace posible introducir las siguientes notaciones para la unión e intersección de una familia de conjuntos:

$$\bigcup_{i=1}^n A_i \equiv A_1 \cup A_2 \cup \cdots \cup A_n, \quad (2.1.1)$$

$$\bigcap_{i=1}^n A_i \equiv A_1 \cap A_2 \cap \cdots \cap A_n. \quad (2.1.2)$$

Se define la diferencia entre dos conjuntos $A - B \equiv A \cap B^c$ como la colección de elementos en A que no están en B . Se tiene que $A - B$, $B - A$ y $A \cap B$ son mutuamente disjuntos. Además,

$$\begin{aligned} A &= (A - B) \cup (A \cap B), \\ B &= (B - A) \cup (A \cap B), \\ A \cup B &= (A - B) \cup (A \cap B) \cup (B - A). \end{aligned} \quad (2.1.3)$$

Por otra parte, la operación de unión distribuye sobre intersección y viceversa:

$$\begin{aligned} A \cap (B \cup C) &= (A \cap B) \cup (A \cap C), \\ A \cup (B \cap C) &= (A \cup B) \cap (A \cup C), \end{aligned} \quad (2.1.4)$$

y más generalmente,

$$\begin{aligned} A \cap \left(\bigcup_{i=1}^n B_i \right) &= \bigcup_{i=1}^n (A \cap B_i), \\ A \cup \left(\bigcap_{i=1}^n B_i \right) &= \bigcap_{i=1}^n (A \cup B_i). \end{aligned} \quad (2.1.5)$$

2.1.5. Espacio Muestral y Eventos

El concepto subyacente en la teoría de la probabilidad es el de *espacio muestral*, que vendría a ser el conjunto universal denotado por \mathcal{S} . Este es la colección de todos los posibles resultados de un experimento. Por ejemplo, para el lanzamiento de una moneda, $\mathcal{S} = \{C, S\}$ ²; para el lanzamiento de dos monedas, $\mathcal{S} = \{CC, CS, SC, SS\}$; y para el lanzamiento de un dado, $\mathcal{S} = \{1, 2, 3, 4, 5, 6\}$.

El espacio muestral de un experimento puede consistir de un número finito o infinito de posibles resultados. Los espacios muestrales finitos son conceptual y matemáticamente simples. Sin embargo, los espacios muestrales con un número infinito de elementos son bastante comunes. Como ejemplo, se puede considerar el lanzamiento de un dardo sobre un blanco rectangular y ver el punto de impacto como el resultado.

Cualquier subconjunto E del espacio muestral se conoce como un *evento*. En otras palabras, un evento es una colección de posibles resultados de un experimento. Así, el evento $\{CS, SC\}$ es descrito como el resultado de lanzar dos monedas, en el que una de las monedas es cara; y $\{2, 4, 6\}$ es el evento de que el lanzamiento de un dado produzca un número par. Un evento, por lo tanto, puede ser *elemental* o *compuesto*, siendo este último una colección del primero.

2.2. Definición clásica

Históricamente, la primera definición de la probabilidad de un evento, fue contar el número de formas en que el evento podría suceder y dividir por el número total de posibles resultados para el experimento. Aquí está implícito que todos los resultados son igualmente posibles.

²C: Cara. S: Sello

Sea A un evento para un experimento con un espacio muestral \mathcal{S} . La probabilidad de A es

$$P(A) = \frac{|A|}{|\mathcal{S}|} = \frac{\text{número de resultados favorables para } A}{\text{número total de resultados en } \mathcal{S}} \quad (2.2.1)$$

Donde se ha usado $|A|$ y $|\mathcal{S}|$ para denotar la cardinalidad o número de elementos de A y \mathcal{S} , respectivamente.

Además,

$$P(A^c) = \frac{|A^c|}{|\mathcal{S}|} = \frac{|\mathcal{S}| - |A|}{|\mathcal{S}|} = 1 - \frac{|A|}{|\mathcal{S}|} = 1 - P(A). \quad (2.2.2)$$

Se debe notar que la probabilidad de un evento es un número entre 0 y 1. Si el evento no puede ocurrir, su probabilidad es 0, en cambio, si es seguro que el evento ocurra su probabilidad es 1.



2.3. Definición de frecuencia relativa

La definición clásica de probabilidad tiene la desventaja de que la expresión “igualmente posible” es vaga. Es más, como esta expresión parece ser sinónimo de “igualmente probable”, la definición es circular, ya que está definiendo probabilidad en términos de probabilidad. Debido a esto, algunas personas han abogado por una definición estadística de probabilidad. De acuerdo con esto, se considera que la probabilidad estimada de un evento es la frecuencia relativa de ocurrencia del evento cuando la cantidad de observaciones es muy grande. La probabilidad misma es el límite de esta frecuencia relativa a medida que la cantidad de observaciones aumenta de manera indefinida.

La definición frecuentista va de la siguiente forma: se supone un experimento, cuyo espacio muestral es \mathcal{S} , que se realiza repetidamente bajo exactamente las mismas condiciones. Para cada evento E del espacio muestral \mathcal{S} , se define $n(E)$ como el número de veces en las primeras n repeticiones del experimento que ocurre el evento E . Así, la probabilidad $P(E)$ del evento E , se define como

$$P(E) = \lim_{n \rightarrow \infty} \frac{n(E)}{n}$$

Esta definición, aunque útil en la práctica, tiene dificultades desde el punto de vista matemático, ya que puede ser que no exista un verdadero límite; ¿Cómo se sabe que $n(E)/n$ convergerá en algún valor límite constante que será el mismo para cada posible secuencia de repeticiones del experimento? Por ejemplo, si el experimento que se realizará repetidamente consiste en lanzar una moneda. ¿Cómo se sabe que la proporción de caras obtenidas en los primeros n lanzamientos convergerá a algún valor a medida que n aumenta? Además, incluso si converge a algún valor, ¿cómo se sabe que, si el experimento se realiza repetidamente por segunda vez, obtendremos la misma proporción límite de caras?

Los defensores de la definición de frecuencia relativa de probabilidad generalmente responden a esta objeción afirmando que la convergencia de $n(E)/n$ a un valor límite constante es una suposición del sistema.

2.4. Definición axiomática

La teoría de probabilidad moderna ha sido desarrollada en forma axiomática; es decir, el concepto de probabilidad se deja sin definir, que es lo mismo que ocurre en la geometría con los conceptos de *punto* y *línea*, que también se dejan sin definir. En concreto, se asume que para cada evento E en el espacio muestral S , existe un valor $P(E)$ referido como la probabilidad de E . Luego se asume que todas estas probabilidades satisfacen un cierto conjunto de axiomas.

A un espacio muestral S y una *función de probabilidad* P se le conoce como un *espacio de probabilidad*. La función P toma un evento $E \subset S$ como entrada y retorna $P(E)$, un número real entre 0 y 1 como resultado. Esta función debe satisfacer los siguientes axiomas

1. *No negatividad:*

$$P(E) \geq 0, \text{ para cada evento } E.$$

2. *Aditividad:*

Si E_1 y E_2 son dos eventos disjuntos, entonces la probabilidad de su unión satisface

$$P(E_1 \cup E_2) = P(E_1) + P(E_2).$$

De forma más general, si el espacio muestral tiene un número infinito de elementos y E_1, E_2, \dots es un secuencia disjunta de eventos, entonces la probabilidad de su unión satisface

$$P\left(\bigcup_i E_i\right) = \sum_i P(E_i)$$

$$P(E_1 \cup E_2 \cup \dots) = P(E_1) + P(E_2) + \dots$$

3. Normalización:

La probabilidad del espacio muestral \mathcal{S} completo es igual a 1, es decir, $P(\mathcal{S}) = 1$.

Cualquier función P que satisfaga estos tres axiomas es considerada una función de probabilidad válida.

La probabilidad tiene las siguientes propiedades para cualesquiera eventos E_1 y E_2 :

1. $P(E_1^c) = 1 - P(E_1)$.
2. Si $E_1 \subseteq E_2$, entonces $P(E_1) \leq P(E_2)$.
3. $P(E_1 \cup E_2) = P(E_1) + P(E_2) - P(E_1 \cap E_2)$. Cuando los eventos E_1 y E_2 no son disjuntos.
4. $P(\emptyset) = 0$. El evento nulo tiene probabilidad cero de que ocurra.

Hasta ahora, no se ha asignado ningún valor a $P(E)$ para un conjunto E dado, y no puede hacerse sin algunos supuestos adicionales sobre las propiedades físicas del espacio muestral y los eventos que lo componen. De hecho, si E_1, E_2, \dots, E_m es una partición de \mathcal{S} , cualquier conjunto no negativo de números p_1, p_2, \dots, p_m que sume 1 con $P(E_i) = p_i$, satisfará los axiomas expuestos. Físicamente, sin embargo, ciertas elecciones no tendrán sentido. Por ejemplo, para $\mathcal{S} = \{C, S\}$, el espacio muestral de una sola moneda, se puede establecer como $P(C) = 0,75$ y $P(S) = 0,25$. Sin embargo, esta asignación no es muy útil para las monedas ordinarias y en la práctica da resultados falsos. Para un espacio muestral compuesto de eventos elementales, es común asignar valores de probabilidad iguales a los eventos elementales. Así, para una moneda $P(C) = P(S) = 0,5$, mientras que para un dado $P(i) = 1/6$, y para una baraja de cartas, $P(E_i) = 1/52$.

2.5. Probabilidades Condicionales y Marginales

En muchas situaciones, el espacio muestral es particionado en formas diferentes. Por ejemplo, un mazo de cartas se puede dividir en 4 pintas o en 13 valores; Los empleados de una empresa pueden dividirse por rangos de edad o por departamentos en los que trabajan. Supóngase que E_1, E_2, \dots, E_m y F_1, F_2, \dots, F_n son dos colecciones de eventos que particionan \mathcal{S} . Esto es, $E_{i_1} \cap E_{i_2} = \emptyset$ con $i_1 \neq i_2$ y $\bigcup_i E_i = \mathcal{S}$; $F_{j_1} \cap F_{j_2} = \emptyset$ con $j_1 \neq j_2$ y $\bigcup_j F_j = \mathcal{S}$. Además, $E_i \cap F_j$, $i = 1, 2, \dots, m$; $j = 1, 2, \dots, n$ también es una partición de \mathcal{S} , y se cumple

$$\bigcup_{j=1}^n (E_i \cap F_j) = E_i \quad \text{y} \quad \bigcup_{i=1}^m (E_i \cap F_j) = F_j. \quad (2.5.1)$$

Dado que $\{E_i\}_{i=1}^m$, $\{F_j\}_{j=1}^n$, y $\{E_i \cap F_j\}_{i=1, j=1}^{m, n}$ son todas particiones de \mathcal{S} , de acuerdo al axioma 2 que debe cumplir una función de probabilidad y la ecuación (2.5.1), se tiene que

$$P(E_i) = \sum_{j=1}^n P(E_i \cap F_j) \quad \text{y} \quad P(F_j) = \sum_{i=1}^m P(E_i \cap F_j). \quad (2.5.2)$$

Donde $P(E_i)$ y $P(F_j)$ son llamadas *probabilidades marginales*.

La probabilidad marginal está asociada con la *probabilidad condicional*. Supóngase que E_i ha ocurrido. ¿Cuál es la probabilidad de F_j ? Por ejemplo, se saca una carta de un mazo de cartas y es un corazón. ¿Cuál es la probabilidad que sea una jota? Esta *probabilidad condicional* se denota por $P(F_j|E_i)$ y es la *probabilidad de F_j dado que E_i ha ocurrido*.

Para entender las probabilidades condicionales y marginales se expondrá un ejemplo. Supóngase una caja que contiene 100 pelotas en tres tamaños diferentes (pequeño, mediano y grande) y en cinco colores diferentes (blanco, negro, rojo, verde y azul). La tabla 2.5.1 muestra la distribución de las pelotas según el color y tamaño.

Si se asume que todos los resultados tienen la misma chance de ocurrir; al sacar una pelota de forma aleatoria la probabilidad de obtener una pelota roja mediana

	Blanco	Negro	Rojo	Verde	Azul	Total
Pequeño	5	7	6	8	4	30
Mediano	8	10	7	12	8	45
Grande	9	5	4	3	4	25
Total	22	22	17	23	16	100

Cuadro 2.5.1: La distribución de pelotas de acuerdo a tamaño y color.

es de 0,07, la de obtener una pelota verde grande es 0,03, y la de obtener de una pelota blanca pequeña es de 0,05. De manera similar, la probabilidad de obtener una pelota negra es de 0,22, y la de obtener una pelota mediana es de 0,45. Con esto presente se puede construir la tabla 2.5.2, que muestra la distribución de las probabilidades según el color y tamaño.

	Blanco	Negro	Rojo	Verde	Azul	Total
Pequeño	0,05	0,07	0,06	0,08	0,04	0,3
Mediano	0,08	0,1	0,07	0,12	0,08	0,45
Grande	0,09	0,05	0,04	0,03	0,04	0,25
Total	0,22	0,22	0,17	0,23	0,16	1

Cuadro 2.5.2: La distribución de probabilidades de acuerdo a tamaño y color.

Cada celda de la última fila y la última columna de la tabla 2.5.2 es lo que se ha llamado probabilidad marginal. La probabilidad condicional de que la pelota sea pequeña *dado que su color es blanco* es $5/22$. Esto se debe a que al restringir el color al blanco, se limita el número de pelotas a 22 en lugar de 100. Del mismo modo, la probabilidad de que la pelota sea verde *dado que su tamaño es mediano* es $12/45$; esto también es una probabilidad condicional. Las probabilidades condicionales se pueden reescribir como razones de probabilidades. Así, la probabilidad de que la pelota sea pequeña dado que su color es blanco es $0,05/0,22$, y la probabilidad de que la pelota sea verde dado que su tamaño es mediano es $0,12/0,45$.

Los resultados del ejemplo anterior pueden generalizarse fácilmente. Sea $p_{ij} = P(E_i \cap F_j)$, construir una tabla con m filas y n columnas, y llenar las celdas con los números p_{ij} . Agregar una fila más para los totales con las entradas $P(F_1)$, $P(F_2)$, hasta $P(F_n)$. Agregar una columna más para los totales con las entradas $P(E_1)$, $P(E_2)$, hasta $P(E_m)$. Ahora debería quedar claro que $P(F_j|E_i)$,

la probabilidad de F_j dado que E_i ha ocurrido, es

$$P(F_j|E_i) = \frac{P(E_i \cap F_j)}{P(E_i)}. \quad (2.5.3)$$

Dado que cualquier evento y su complemento particionan el conjunto universal, se puede hacer $F_1 = A$ y $F_2 = A^c$, y con esto la ecuación anterior queda como

$$P(A|E_i) = \frac{P(E_i \cap A)}{P(E_i)}, \quad (2.5.4)$$

o si se tienen dos conjuntos A y B (y sus complementos) que particionan \mathcal{S} , entonces

$$P(A|B) = \frac{P(B \cap A)}{P(B)}, \quad (2.5.5)$$

lo que se cumple para *cualesquiera dos* conjuntos.

Si la probabilidad $P(A|B)$ no depende del evento B de ninguna manera, es decir, si $P(A|B) = P(A)$, entonces se dice que los dos eventos A y B son *estadísticamente independientes*. La ecuación (2.5.5) ahora produce

$$P(A) = \frac{P(B \cap A)}{P(B)}$$

o

$$P(A \cap B) = P(A)P(B) \quad (2.5.6)$$

y esta última ecuación se convierte en la definición de dos eventos estadísticamente independientes.

Es importante diferenciar entre independencia estadística y exclusión mutua³. Si dos eventos son mutuamente excluyentes, entonces tienen que ser estadísticamente *dependientes* ya que la ocurrencia de uno impide la ocurrencia del otro. Del mismo modo, la ecuación (2.5.6) muestra que si $P(A) > 0$, $P(B) > 0$, y A y B son estadísticamente independientes, entonces si $P(A \cap B) = 0$ implica que $A \cap B = \emptyset$, por lo tanto, A y B no pueden ser mutuamente excluyentes.

³Eventos disjuntos.

La ecuación (2.5.4) puede ser reescrita como

$$P(A \cap E_i) = P(E_i)P(A|E_i),$$

y si $A \cap E_i$ son mutuamente excluyentes y su unión es A , se tiene⁴

$$P(A) = \sum_{i=1}^m P(E_i)P(A|E_i). \quad (2.5.7)$$

Lo que se conoce como *teorema de Bayes*.



⁴Ver ecuación (2.5.2) con $A = F_j$

Capítulo 3

Mecánica Cuántica

A principios del siglo XX había un conjunto de problemas fundamentales para los cuales la física clásica no tenía respuesta. Estos problemas no podían ser analizados en el contexto de las teorías físicas existentes.

La crisis que se produjo logró sacudir la convicción imperante a fines del siglo XIX, de que la física era una ciencia prácticamente completa en lo que a principios se refiere, y obligó a reconocer la necesidad de un cambio en la concepción del mundo físico. Esto llevó a la aparición de la mecánica cuántica [4].

La mecánica cuántica difiere de la mecánica clásica, y una de las diferencias se manifiesta en el proceso de medición. En la teoría clásica se asume que al medir, las propiedades del sistema se mantienen sin cambios, en cambio en la teoría cuántica, la medición tiene resultados aleatorios y perturban el estado del sistema. Por esta razón cuando se habla de la descripción del estado de un sistema cuántico, esto se refiere a: la posibilidad de predecir probabilísticamente los resultados de la medición (de magnitudes) del sistema.

Otra de las diferencias importantes entre la mecánica clásica y la mecánica cuántica es el formalismo. Por sí sola, la teoría cuántica no dice las leyes concretas que gobiernan la evolución e interacción de los sistemas [5].

En este capítulo se presentan nociones de álgebra lineal necesarios para presentar los postulados y el formalismo de la mecánica cuántica. Está basado principalmente en [5] y toma elementos de [6, 7].

3.1. Espacio de Hilbert

Dado que se trabajará con sistemas finitos, es suficiente entender un *espacio de Hilbert* como un espacio vectorial complejo de dimensión finita con producto escalar.

Se debe notar que en el contexto de la mecánica cuántica los elementos del espacio vectorial son la forma de representar un sistema, y las cantidades físicas que se quieren medir se representan mediante operadores que actúan sobre los vectores o elementos del espacio de Hilbert.

Para dos vectores

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix}, \quad |\phi\rangle = \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix},$$

pertenecientes a un espacio de Hilbert \mathcal{H} de n dimensiones, el *producto interior*¹ viene dado por

$$(|\psi\rangle, |\phi\rangle) = \langle\psi|\phi\rangle = \begin{pmatrix} \psi_1 & \dots & \psi_n \end{pmatrix} \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} = \sum_{i=1}^n \psi_i^* \phi_i.$$

De aquí se desprende que el producto interior de $|\psi\rangle$ con sí mismo es

$$\| |\psi\rangle \|^2 = \langle\psi|\psi\rangle = \sum_{i=1}^n |\psi_i|^2, \quad (3.1.1)$$

que es real positivo y solo es cero cuando $|\psi\rangle = \vec{0}$.

Se debe notar que:

- Un vector se dice *normalizado* si el producto interior con sí mismo es 1.
- Dos vectores son *ortogonales* si el producto interior entre ellos es 0.
- Un conjunto de vectores $\{|\psi_n\rangle\}$ son *ortonormales* si ellos son normalizados

¹O producto escalar

y mutuamente ortogonales, es decir:

$$\langle \psi_m | \psi_n \rangle = \delta_{nm}. \quad (3.1.2)$$

- $\langle \psi | \phi \rangle = \langle \phi | \psi \rangle^*$

3.2. Operadores Lineales y Matrices

Los operadores que actúan sobre un espacio de Hilbert mapean un vector en otro vector del espacio, esto es, son *transformaciones lineales* que pueden ser representadas por matrices:

$$|\phi\rangle = A|\psi\rangle \Leftrightarrow \begin{pmatrix} \phi_1 \\ \vdots \\ \phi_n \end{pmatrix} = \begin{pmatrix} A_{11} & \dots & A_{1n} \\ \vdots & \dots & \vdots \\ A_{n1} & \dots & A_{nn} \end{pmatrix} \begin{pmatrix} \psi_1 \\ \vdots \\ \psi_n \end{pmatrix}. \quad (3.2.1)$$

Por otro lado, del álgebra lineal se sabe que un *operador lineal* entre espacios vectoriales V y W se define como $A : V \longrightarrow W$,

$$A\left(\sum_i a_i |\psi\rangle\right) = \sum_i a_i A(|\psi\rangle). \quad (3.2.2)$$

Ahora bien, supóngase que V , W y X son espacios vectoriales, $A : V \longrightarrow W$ y $B : W \longrightarrow X$ son operadores lineales. A partir de esto se define explícitamente la composición de operadores, en particular, BA denota la composición de B con A . De esta forma, se puede generalizar la acción sobre el espacio con una n -ésima composición de operadores.

Una relación extremadamente útil es la relación de completitud,

$$I = \sum_i |i\rangle\langle i|, \quad (3.2.3)$$

donde I es el operador identidad, es decir, $I|\psi\rangle = |\psi\rangle$ para cualquier $|\psi\rangle$. La suma de la derecha es sobre diadas $|i\rangle\langle i|$ correspondiente a los elementos $|i\rangle$ de una base ortonormal.

Usando (3.2.3) se tiene que:

$$|\psi\rangle = \left(\sum_i |i\rangle\langle i| \right) |\psi\rangle = \sum_i |i\rangle \langle i|\psi\rangle = \sum_i \langle i|\psi\rangle |i\rangle. \quad (3.2.4)$$

Los operadores también pueden ser representados por matrices, en efecto, dado un operador A y una base $\{v_i\}$ que no necesariamente es ortonormal, se le puede asociar una matriz cuadrada A de números definidos por A_{ij} :

$$A|v_j\rangle = \sum_i |v_i\rangle A_{ij} = \sum_i A_{ij} |v_i\rangle. \quad (3.2.5)$$

La matriz depende de la elección de la base, así como en el operador. En el caso de una base ortonormal y utilizando (3.2.3) se tiene,

$$A|j\rangle = IA|j\rangle = \left(\sum_i |i\rangle\langle i| \right) A|j\rangle = \sum_i |i\rangle \langle i|A|j\rangle = \sum_i \langle i|A|j\rangle |i\rangle, \quad (3.2.6)$$

donde $\langle i|A|j\rangle$ es el producto interior de $|i\rangle$ con $A|j\rangle$, equivalente a A_{ij} en la expresión (3.2.5). Así, $\langle i|A|j\rangle$ se conoce como un *elemento de matriz* cuando se utiliza la notación de Dirac.

Cuando A se refiere a un qubit², la forma habitual de escribir la matriz en la base estándar³ es:

$$\begin{pmatrix} \langle 0|A|0\rangle & \langle 0|A|1\rangle \\ \langle 1|A|0\rangle & \langle 1|A|1\rangle \end{pmatrix}.$$

Nótese el orden de los elementos.

Otra aplicación de (3.2.3) está en escribir el elemento de matriz del producto de dos operadores en términos de los elementos matriciales individuales:

$$\langle i|AB|j\rangle = \langle i|AIB|j\rangle = \sum_m \langle i|A|m\rangle \langle m|B|j\rangle, \quad (3.2.7)$$

²Por el momento se entenderá como un vector de dos dimensiones.

³O base computacional o base lógica: $|0\rangle, |1\rangle$.

usando subíndices, la ecuación anterior queda de la forma:

$$(AB)_{ij} = \sum_m A_{im} B_{mj}. \quad (3.2.8)$$

Adicionalmente, la *traza* $\text{Tr}(A)$ de un operador A es la suma de los elementos diagonales de esta matriz, es decir:

$$\text{Tr}(A) = \sum_i \langle i|A|i\rangle = \sum_i A_{ii}. \quad (3.2.9)$$

La traza es independiente de la base utilizada en la definición de los elementos de matriz, en particular, no se necesita usar una base ortonormal.

3.2.1. Operadores adjuntos y hermíticos

Supóngase un operador A actuando sobre un espacio de Hilbert \mathcal{H} , existe un operador lineal único A^\dagger sobre \mathcal{H} de tal manera que, para todos los vectores $|\psi\rangle$ y $|\phi\rangle \in \mathcal{H}$,

$$(|\psi\rangle, A|\phi\rangle)^* = \langle\psi|(A|\phi\rangle) = (\langle\phi|A^\dagger|\psi\rangle) = (A^\dagger|\phi\rangle, |\psi\rangle), \quad (3.2.10)$$

este operador lineal es conocido como el *adjunto* o el *hermítico conjugado* del operador A , además, $(AB)^\dagger = B^\dagger A^\dagger$. Por convención, si $|\phi\rangle$ es un vector, se define $|\phi\rangle^\dagger \equiv \langle\phi|$, de lo cual se desprende $(A|\phi\rangle)^\dagger = \langle\phi|A^\dagger$.

Se debe tener en consideración que la operación daga es antilineal, esto es, los escalares se sustituyen por sus complejos conjugados.

Un *operador normal* A sobre un espacio de Hilbert es uno que conmuta con su adjunto, es decir, $AA^\dagger = A^\dagger A$. Ellos tienen la propiedad de ser diagonalizados usando una base ortonormal, de la forma:

$$A = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i| \quad (3.2.11)$$

donde los vectores $|\lambda_i\rangle$ son *autovectores*⁴ de A y los λ_i son sus *autovalores*⁵.

⁴También llamados vectores propios.

⁵También llamados valores propios.

Equivalentemente, la matriz de A en esta base es diagonal,

$$\langle \lambda_i | A | \lambda_j \rangle = \lambda_i \delta_{ij}. \quad (3.2.12)$$

La ecuación (3.2.11) es conocida como la *forma espectral del operador* A y al conjunto de autovalores $\{\lambda_i\}$ se le llama *espectro del operador*. Ahora bien, un *operador hermítico*⁶ definido por la propiedad $A = A^\dagger$ es también un operador normal, siendo el análogo de un número real (en oposición a un complejo). Sus autovalores λ_i son números reales.

También existe un operador llamado *proyector* o más formalmente, *operador proyección ortogonal*, que satisface $P^2 = P$. Este es un operador hermítico con autovalores 0 o 1, por lo tanto, siempre hay una base (que depende, por supuesto, del proyector) en la que su matriz es diagonal en el sentido de (3.2.12), con solo 0 o 1 en la diagonal principal.

3.2.2. Operadores Unitarios

Los *operadores unitarios* U tienen la propiedad:

$$U^\dagger U = I = U U^\dagger. \quad (3.2.13)$$

Donde se ve que U conmuta con su adjunto, por lo que además es un operador normal y se puede escribir en la forma (3.2.11). Luego, de (3.2.13) se tiene la condición: todos los autovalores de U son números complejos de magnitud 1, es decir, se encuentran en la circunferencia unitaria en el plano complejo.

Además, se debe notar que la acción de operadores unitarios preserva el producto interno entre vectores, de modo que si $|v\rangle$ y $|w\rangle$ son dos vectores en un espacio de Hilbert \mathcal{H} y $|v'\rangle = U|v\rangle$ y $|w'\rangle = U|w\rangle$ con U unitaria, entonces

$$\langle v' | w' \rangle = \langle v | U^\dagger U | w \rangle = \langle v | I | w \rangle = \langle v | w \rangle.$$

Esto significa que dada una base ortonormal $\{|v_n\rangle\}$, los vectores $|w_n\rangle = U|v_n\rangle$ también son una base ortonormal.

⁶También conocido como autoadjunto

En un espacio de Hilbert de dimensión finita, con U mapeando el espacio sobre sí mismo, cada igualdad en (3.2.13) implica la otra, por lo que basta solo considerar una de ellas, $UU^\dagger = I$, para verificar si U es unitario.

Finalmente, en mecánica cuántica se utilizan operadores unitarios para cambiar de una base ortonormal a otra, para representar simetrías como la de rotación y para describir algunos aspectos de la dinámica o la evolución de un sistema cuántico.

3.2.3. Operadores de Pauli

Los *operadores de Pauli*⁷ son operadores hermíticos actuando sobre un espacio de Hilbert de 2 dimensiones. A estos se les designa por el símbolo σ_i con $i = 1, 2, 3$ o $i = x, y, z$:

$$\sigma_i^\dagger = \sigma_i, \quad (3.2.14)$$

y además satisfacen la condición, $\sigma_i^2 = I$.

Si se considera la hermiticidad del operador, se puede ver que sus autovalores son $+1$ y -1 . Al mismo tiempo, se puede observar por su descomposición espectral que σ_i es unitario,

$$\sigma_k^\dagger = \sigma_k^{-1} \quad (3.2.15)$$

y su traza $\text{Tr}(\sigma_k)$ es nula.

Además, estos operadores satisfacen relaciones de anticonmutación, $\{A, B\} = AB + BA$

$$\{\sigma_i, \sigma_j\} = 2\delta_{ij}I. \quad (3.2.16)$$

Existe otra propiedad importante de los σ_i que viene dada por el conmutador

⁷También se les conoce como matrices de Pauli.

$([A, B] = AB - BA)$ y es complementaria a la relación (3.2.16)

$$[\sigma_i, \sigma_j] = 2i \sum_{k=1}^3 \epsilon_{ijk} \sigma_k, \quad (3.2.17)$$

con ϵ_{ijk} el símbolo de Levi-Civita⁸. Finalmente y en adición a las ecuaciones (3.2.16) y (3.2.17) se puede escribir:

$$\sigma_i \sigma_j = \delta_{ij} I + i \sum_{k=1}^3 \epsilon_{ijk} \sigma_k. \quad (3.2.18)$$

3.2.3.1. Representación matricial

Si considera una base ortonormal de autovectores $|0\rangle$ y $|1\rangle$ de σ_z con autovalores $+1$ y -1 respectivamente, se ve que:

$$\begin{aligned} \sigma_z |0\rangle &= +|0\rangle \\ \sigma_z |1\rangle &= -|1\rangle. \end{aligned}$$

Por consiguiente, en la base computacional la representación matricial de σ_z es:

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \quad (3.2.19)$$

Usando las ecuaciones (3.2.14) y (3.2.18) se encuentran las expresiones para σ_x y σ_y , completando el conjunto de las denominadas matrices de Pauli,

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = |0\rangle\langle 1| + |1\rangle\langle 0|, \quad (3.2.20)$$

$$\sigma_y = \begin{pmatrix} 0 & -1 \\ i & 0 \end{pmatrix} = -i(|0\rangle\langle 1| - |1\rangle\langle 0|), \quad (3.2.21)$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|. \quad (3.2.22)$$

⁸ $\epsilon_{ijk} = 1$ si (i, j, k) es $(1, 2, 3)$, $(2, 3, 1)$, o $(3, 2, 1)$; $\epsilon_{ijk} = -1$ si (i, j, k) es $(3, 2, 1)$, $(1, 3, 2)$, o $(2, 1, 3)$; $\epsilon_{ijk} = 0$ si $i = j$, o $j = k$, o $k = i$.

Por otra parte, la acción de los operadores σ_i sobre los vectores de la base computacional se muestra a continuación:

$$\sigma_x |0\rangle = |1\rangle \quad (3.2.23a)$$

$$\sigma_x |1\rangle = |0\rangle \quad (3.2.23b)$$

$$\sigma_y |0\rangle = +i |1\rangle \quad (3.2.23c)$$

$$\sigma_y |1\rangle = -i |0\rangle \quad (3.2.23d)$$

$$\sigma_z |0\rangle = + |0\rangle \quad (3.2.23e)$$

$$\sigma_z |1\rangle = - |1\rangle \quad (3.2.23f)$$

donde σ_x hace un cambio de estado (*bit flip*), σ_y intercambia e introduce la fase $\pm i$, y σ_z introduce la fase ± 1 (*phase flip*).

3.3. Postulados de la Mecánica Cuántica

La mecánica cuántica es un marco matemático para el desarrollo de teorías físicas. Por sí misma, la mecánica cuántica no dice qué leyes un sistema físico debe obedecer, pero provee un marco matemático y conceptual para el desarrollo de tales leyes. Los postulados proveen una conexión entre el mundo físico y el formalismo matemático de la mecánica cuántica.

Los postulados de la mecánica cuántica fueron derivados después de un largo proceso de ensayo y error, que implicó una considerable cantidad de conjeturas y dudas por parte de los creadores de la teoría, y pesar de más de un siglo de investigación, numerosas preguntas relacionadas con los fundamentos de la mecánica cuántica siguen sin resolver. Por ejemplo, hasta ahora no se ha encontrado una explicación satisfactoria para el hecho de que la mecánica cuántica tenga su particular estructura matemática, como consecuencia, algunos de los aspectos que se discutirán a continuación, a saber, los postulados de la mecánica cuántica pueden parecer carentes de una motivación clara.

En esta sección, describiremos uno de los enfoque estándar de la mecánica cuántica.

Está basado en un número de postulados formulados por Dirac y von Neumann con respecto a los estados de los sistemas físicos [6], así como a su evolución. Los postulados son los siguientes:

3.3.0.1. Postulado 1: Estados

Asociado a cualquier grado de libertad de un sistema físico aislado hay un espacio de Hilbert \mathcal{H} , conocido como *espacio de estados*. El sistema es completamente descrito por su *vector de estado* $|\psi\rangle$, que es un vector unitario del espacio de estados \mathcal{H} .

Este primer postulado establece el escenario en el que tiene lugar la descripción matemática de la mecánica cuántica, sin embargo no dice nada con respecto a cómo construir el espacio de Hilbert asociado al sistema.

3.3.0.2. Postulado 2: Dinámica

La evolución de un sistema cuántico cerrado es descrita por medio de una transformación unitaria. El estado $|\psi(t_0)\rangle$ del sistema está relacionado con el estado $|\psi(t)\rangle$ por un operador unitario U que depende solo de los tiempos t_0 y t ,

$$|\psi(t)\rangle = U(t_0, t) |\psi(t_0)\rangle. \quad (3.3.1)$$

De la misma manera que el primer postulado no dice cuál es el espacio de estados o el vector de estado de un sistema, el segundo postulado no dice qué operadores unitarios U describen la dinámica cuántica de un sistema real. Este postulado solo asegura que la evolución de cualquier sistema cuántico cerrado puede describirse de esa forma.

3.3.0.3. Postulado 3: Observables

Se conoce como *observable* a cualquier propiedad física que pueda ser medida en un sistema. Todos los observables son representados por operadores hermíticos actuando sobre el espacio de estados \mathcal{H} , y cada autovalor de este operador corresponde a un posible resultado de medir dicho observable.

Si el espectro del operador es discreto, entonces los resultados que pueden ser obtenidos de la medición de dicho observable están cuantizados.

3.3.0.4. Postulado 4: Mediciones

La medición⁹ de un observable O produce un autovalor λ_i . Si el sistema está en el estado $|\psi\rangle \in \mathcal{H}$, entonces la probabilidad de obtener el resultado λ_i es dada por la *regla de Born*:

$$P(\lambda_i) = |\langle \phi | \psi \rangle|^2, \quad (3.3.2)$$

con $|\phi\rangle$ un autovector normalizado asociado al observable O con autovalor λ_i .

Además, el estado $|\psi'\rangle$ del sistema después de la medición, condicionado al evento de que el resultado es λ_i , es dado por

$$|\psi'\rangle = \sqrt{\frac{1}{P(\lambda_i)}} \hat{P}_{\lambda_i} |\psi\rangle, \quad (3.3.3)$$

con \hat{P}_{λ_i} el proyector propio de O asociado al autovalor¹⁰ λ_i .

3.3.0.5. Postulado 5: Composición

Para N sistemas físicos con espacios de estado \mathcal{H}_i , $i = 1, 2, \dots, N$, el espacio de estados de considerar el conjunto de sistemas es $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_N$. Además, si los sistemas individuales están en estados $|\psi_1\rangle \in \mathcal{H}_1$, $|\psi_2\rangle \in \mathcal{H}_2$, ..., $|\psi_N\rangle \in \mathcal{H}_N$ entonces el estado conjunto es¹¹

$$|\Psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_N\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \dots \otimes \mathcal{H}_N. \quad (3.3.4)$$

3.4. Operador Densidad

En la sección anterior se escribieron los postulados de la mecánica cuántica usando vectores de estado. Una formulación alternativa es posible usando el *operador densidad* o también conocido como *matriz densidad*. Esta formulación alternativa es matemáticamente equivalente al enfoque de vectores de estado.

El lenguaje del operador densidad proporciona una manera conveniente para

⁹Caso de un espectro discreto no degenerado.

¹⁰Como \hat{P}_{λ_i} es proyector propio se tiene que $O\hat{P}_{\lambda_i} = \lambda_i\hat{P}_{\lambda_i}$.

¹¹También se puede escribir $|\psi_1\rangle |\psi_2\rangle \dots |\psi_N\rangle$ o $|\psi_1\psi_2 \dots \psi_N\rangle$ en lugar de $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \dots \otimes |\psi_N\rangle$.

describir sistemas cuánticos cuyo estado no se conoce completamente. Más precisamente, supóngase un sistema cuántico en uno de los posibles estados $|\psi_i\rangle$, donde cada estado tiene una probabilidad p_i asociada. El conjunto de probabilidades y estados puros $\{p_i, |\psi_i\rangle\}$ es conocido como un *ensemble de estados puros*. El operador densidad para el sistema se define por la ecuación

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|. \quad (3.4.1)$$

Cabe notar que si se usa el lenguaje del operador densidad o el lenguaje de los vectores de estado es un asunto de gustos, dado que ambos conducen a los mismos resultados, sin embargo a veces es mucho más fácil abordar problemas desde un punto de vista que desde el otro.

Además, es importante señalar que un sistema cuántico cuyo estado $|\psi\rangle$ es conocido de forma exacta se dice que está en un *estado puro*. En este caso el operador densidad es simplemente $\rho = |\psi\rangle\langle\psi|$. De otro modo, ρ es un *estado mixto*¹², es decir, que es una mezcla de los diferentes estados puros en el ensemble para ρ .

Un operador densidad debe cumplir las siguientes condiciones:

- Condición de normalización.

$$\text{Tr}(\rho) = 1, \quad (3.4.2)$$

es decir, la suma de los elementos diagonales es igual a 1.

- Condición de positividad.

$$\langle\phi|\rho|\phi\rangle \geq 0, \quad (3.4.3)$$

para cualquier vector $|\phi\rangle$ en el espacio de estados.

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

$$\rho = \sum_j \lambda_j |j\rangle\langle j|, \quad (3.4.4)$$

¹²O estado mezcla.

donde los vectores $|j\rangle$ son mutuamente ortogonales y los valores propios de ρ , λ_j son reales positivos.

En general, para la traza de un operador densidad se cumple que $\text{Tr}(\rho^2 \leq 1)$. La igualdad se satisface solo para estados puros, por lo que la expresión anterior es utilizada como un criterio para cualificar la pureza de un estado cuántico. Además, el operador densidad es hermítico.

3.5. Reformulación de los Postulados

3.5.0.1. Postulado 1: Estados

En un tiempo fijo t_0 el estado del sistema físico es completamente descrito por un operador densidad, el cual es positivo con traza unitaria, actuando sobre el espacio de estados del sistema. En efecto, si el sistema cuántico está en el estado ρ_i con probabilidad p_i , entonces, el operador densidad para el sistema es:

$$\sum_i p_i \rho_i. \quad (3.5.1)$$

3.5.0.2. Postulado 2: Dinámica

La evolución de un sistema cuántico cerrado es descrita por una transformación unitaria. Tal que, el estado ρ en el tiempo t_1 se relaciona con el estado ρ' del sistema en el tiempo t_2 mediante un operador unitario U ,

$$\rho' = U\rho U^\dagger. \quad (3.5.2)$$

3.5.0.3. Postulado 3: Mediciones

Una medición es descrita por un conjunto de *operadores de medida* $\{M_m\}$. El subíndice m indica el resultado de la medición. Si el estado del sistema inmediatamente antes de la medición es ρ , entonces la probabilidad de obtener el resultado m es:

$$p(m) = \text{Tr}(M_m^\dagger M_m \rho) \quad (3.5.3)$$

y el estado inmediatamente después de la medición es

$$\frac{M_m^\dagger \rho M_m}{\text{Tr}(M_m^\dagger M_m \rho)}. \quad (3.5.4)$$

Los operadores que permiten realizar procesos de medida satisfacen la condición de completitud,

$$\sum_m M_m^\dagger M_m = 1. \quad (3.5.5)$$

3.5.0.4. Postulado 4: Composición

El estado de un sistema físico compuesto es el producto tensorial de los estados físicos que lo componen. Además, si tenemos sistemas numerados del 1 hasta el N , y el sistema i se prepara en el estado ρ_i , entonces, el sistema total es¹³ $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_N$.



¹³También se puede escribir $\rho_1 \rho_2 \dots \rho_N$ en lugar $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_N$

Capítulo 4

Teoría de la Información Cuántica

“Una teoría de la información basada en los principios cuánticos, amplía y completa la teoría clásica de la información, del mismo modo que los números complejos amplían y completan los reales.”

(Bennett et al., 2000, p. 247)[8].

“El campo de la información cuántica no tiene que ver con los problemas fundamentales, en lugar de eso, se basa en la validez de la mecánica cuántica y aplica los rasgos características de los sistemas entrelazados para diseñar esquemas nuevos y potentes para la comunicación y computación.” (Alber et al., 2001, p. 59)[9].

4.1. Qubit

El *bit* es un concepto fundamental en teoría de la información clásica, esto hace necesario introducir un concepto análogo en teoría de la información cuántica [10]: el *bit cuántico* o comúnmente llamado *qubit* [5].

Un bit es un sistema que puede estar en uno de dos estados posibles, ya sea 0 ó 1¹. De la misma forma, un qubit también puede adoptar uno de dos posibles estados: $|0\rangle$ o $|1\rangle$, pero a diferencia de los bits clásicos, un qubit puede además estar en una *superposición* de estos dos estados, es decir,

$$|\psi\rangle = a|0\rangle + b|1\rangle \quad (4.1.1)$$

¹Representados así en el sistema binario.

con $a, b \in \mathbb{C}$ y $|a|^2 + |b|^2 = 1$.

Dicho de otra forma, un qubit es un vector en un espacio de Hilbert de dos dimensiones y los estados $|0\rangle$ y $|1\rangle$ forman una base ortonormal para este espacio vectorial. Una forma conveniente de visualizar un qubit es dada en la siguiente representación geométrica.

Dado que $|a|^2 + |b|^2 = 1$, es posible reescribir la ecuación (4.1.1) como

$$|\psi\rangle = e^{i\gamma} \left(\cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \right), \quad (4.1.2)$$

donde θ, φ y γ son números reales y $e^{i\gamma}$ es una fase global que podemos ignorar, ya que no produce efectos observables. De esta forma, se puede escribir

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\varphi} \sin \frac{\theta}{2} |1\rangle \quad (4.1.3)$$

Es claro que los números θ y φ definen un punto sobre una esfera unitaria tridimensional, como se muestra en la figura 4.1.1.

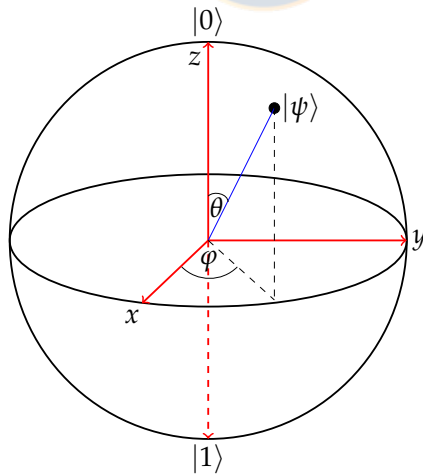


Figura 4.1.1: Representación de Esfera de Bloch de un qubit. *Fuente: Elaborado por el autor.*

Esta esfera es comúnmente llamada *esfera de Bloch* y es una herramienta útil para visualizar qubits individuales y describir muchas de las operaciones que se aplican a ellos, sin embargo hay que tener en cuenta que es limitada, porque no

hay generalizaciones simples conocidas de la esfera de Bloch para múltiples qubits.

Ahora bien ¿cuánta información es representada por un qubit? Paradójicamente, hay un número infinito de puntos sobre la esfera unitaria, de manera que en principio podríamos almacenar un texto completo de Heidegger en la expansión binaria infinita de θ , sin embargo, esta afirmación resulta ser engañosa, debido al comportamiento del qubit cuando es observado [5]. Se debe recordar que la medición de un qubit dará solo 0 ó 1, además de cambiar el estado del sistema. Por ejemplo, considérese el estado

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

si la medición de $|+\rangle$ da 0, entonces el estado post-medición del qubit será $|0\rangle$, perdiendo la superposición que permitía almacenar infinita información.

Por lo tanto, *a partir de una sola medición se obtiene únicamente un bit de información sobre el estado del qubit* [11].

4.1.1. Múltiples qubits

Supóngase se tienen dos qubits. Si estos fueran bits clásicos, entonces habría cuatro posibles estados, a saber, 00, 01, 10 y 11. Correspondientemente, un sistema de dos qubits tiene cuatro estados bases denotados $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$. También puede existir un par de qubits en una superposición de estos cuatro estados, por lo que el estado cuántico de dos qubits implica asociar un coeficiente complejo² con cada estado de la base [5], de modo que el vector de estado que describe los dos qubits es

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \quad (4.1.4)$$

con las amplitudes complejas limitadas solo por la condición de normalización $|a_{00}|^2 + |a_{01}|^2 + |a_{10}|^2 + |a_{11}|^2 = 1$.

La generalización resulta natural cuando se tiene n qubits [12], el estado general

²También llamado amplitud de probabilidad.

ahora puede escribirse como la superposición de los 2^n estados base $|x_n\rangle^3$ diferentes con amplitudes cuyos módulos al cuadrado suman 1:

$$|\psi\rangle = \sum_{0 \leq x \leq 2^n} a_x |x_n\rangle, \quad (4.1.5)$$

$$\sum_{0 \leq x \leq 2^n} |a_x|^2 = 1. \quad (4.1.6)$$

De esta forma se ha definido el elemento básico de la teoría de la información cuántica.

4.2. Entropía de von Neumann

La *entropía de von Neumann* de un estado cuántico con operador densidad ρ se define como [7]

$$S(\rho) = -\text{Tr}(\rho \log_2 \rho). \quad (4.2.1)$$

Se puede calcular dicha entropía en términos de los autovalores del operador densidad

$$\rho = \sum_i \lambda_i |\lambda_i\rangle\langle\lambda_i|,$$

luego,

$$\log_2 \rho = \sum_j \log_2(\lambda_j) |\lambda_j\rangle\langle\lambda_j|.$$

De esta forma al trazar utilizando como base los autovectores del operador densidad, se obtiene

$$S(\rho) = \sum_i -\lambda_i \log_2 \lambda_i, \quad (4.2.2)$$

donde se define que $0 \log_2 = 0$.

³ x_n representa una cadena de 0s y 1s de largo n . Así, para $n = 2$ se tiene que x_n toma los valores del conjunto $\{00, 01, 10, 11\}$.

La entropía de von Neumann es la versión cuántica de la *entropía de Shannon* clásica [7]. Para una variable discreta X que puede tomar un valor x con probabilidad p_x , la entropía de Shannon se define como [5]

$$H(X) = - \sum_x p_x \log_x p_x. \quad (4.2.3)$$

Similar a la entropía de Shannon, que mide la incertidumbre de una variable aleatoria clásica, la entropía de von Neumann mide la incertidumbre de un estado cuántico [13].

Los estados puros representan el conocimiento completo acerca de un sistema cuántico: su entropía de von Neumann es cero. Por otro lado, para un espacio de Hilbert de d dimensiones, la incertidumbre máxima está representada por el operador densidad mixto $\rho = \frac{1}{d}I_{d \otimes d}$ con entropía de von Neumann $\log_2 d$. Además, la entropía de von Neumann es no negativa para cualquier operador densidad [5, 7].

Por otro lado, es de suma importancia destacar que la entropía de un operador densidad es invariante bajo transformaciones unitarias, esto es

$$S(\rho) = S(U\rho U^\dagger), \quad (4.2.4)$$

con U un operador unitario y U^\dagger su hermítico conjugado.

Además, en ocasiones es necesario determinar una cantidad de una sola parte de un sistema multipartito. Por ejemplo: considérese un sistema cuántico compuesto de dos partes⁴, el cual se encuentra en un estado puro $|\psi_{AB}\rangle$. Luego, los estados del subsistema A y B vienen dados por

$$\begin{aligned} \rho_A &= \text{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|), \\ \rho_B &= \text{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|). \end{aligned}$$

Dado que el estado del sistema cuántico bipartito se encuentra en un estado puro, su entropía de von Neumann es cero, sin embargo la entropía de von Neumann de

⁴También se les denomina sistemas bipartitos.

los subsistemas A y B no necesariamente es nula. De esta forma

$$\begin{aligned} S(A) &\geq 0, \\ S(B) &\geq 0. \end{aligned}$$

Adicionalmente, como el sistema está en un estado puro, se cumple la siguiente propiedad:

$$S(\rho_A) = S(\rho_B). \quad (4.2.5)$$

La demostración se basa en que todo estado puro de un sistema bipartito puede escribirse utilizando la descomposición de Schmidt [5].

Al trazar parcialmente sobre el estado bipartito se debe notar que, los autovalores de ρ_A y ρ_B son iguales, lo que implica que sus entropías de von Neumann también lo son. La propiedad es válida para sistemas multipartitos siempre cuando el estado del sistema completo sea un estado puro [7].

4.3. Entrelazamiento

Por mucho tiempo, el entrelazamiento fue visto solo como uno de los rasgos contraintuitivos de la mecánica cuántica, solo importante dentro del contexto de la paradoja EPR. Es en estas últimas décadas que el campo de la información cuántica ha explotado estas características para obtener nuevos tipos de transmisión y procesamiento de la información [9].

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 juega un rol fundamental en distintas aplicaciones de computación cuántica [14, 15, 16] e información cuántica, tales como: preparación remota de estado [17, 18, 19], codificación superdensa [20], teleportación de estados cuánticos [21], intercambio de entrelazamiento [22] y criptografía cuántica [23].

4.3.1. Revisión del concepto

La siguiente revisión del concepto de entrelazamiento está basada en [24].

En el año 1935 E. Schrödinger se refirió al entrelazamiento como “el rasgo característico de la mecánica cuántica” [25]. En efecto, al hacer interactuar dos sistemas (que en un inicio están separados espacialmente y tienen estados bien definidos) mediante fuerzas conocidas, y luego de un tiempo finito de influencia mutua separarlos, estos ya no podrán ser descritos de la misma forma inicial, es decir, ya no podrán ser especificados de manera independiente cada uno de ellos. Esta es una de las características de la teoría cuántica que genera un distanciamiento notable de las líneas del pensamiento clásico. Debido a la interacción los sistemas cambian, se conectan, se entrelazan.

Paralelamente el mismo año, la interpretación de Copenhague de la mecánica cuántica era fuertemente criticada por A. Einstein, B. Podolsky y N. Rosen (EPR) [26]. En el trabajo que publicaron, ellos cuestionan (bajo su propio paradigma de realidad) si la mecánica cuántica puede ser considerada una teoría completa de la realidad física; Plantean que en una teoría completa, cada elemento de la realidad física debe tener una contraparte en la teoría, de esta forma la mecánica cuántica debería satisfacer el criterio siguiente:

“Si, sin perturbar en ningún modo un sistema, se puede predecir con certeza (es decir, con probabilidad igual a uno) el valor de una cantidad física, entonces existe un elemento de realidad física correspondiente a dicha cantidad física.” (Einstein et al., 1935, p. 777)[26].

El argumento EPR señala que en mecánica cuántica, si los operadores A y B correspondientes a dos cantidades físicas no conmutan, esto es $AB \neq BA$, entonces el conocimiento preciso de una de las cantidades excluye el conocimiento de la otra. Por lo tanto, se concluye que:

- i) la descripción de la realidad de la mecánica cuántica entregada por la función de onda no es completa, o
- ii) cuando los correspondientes operadores de dos cantidades físicas no conmutan, no pueden tener realidad simultáneamente.

Posteriormente en el mismo año, N. Bohr [27] respondió a la crítica realizada a la interpretación de Copenhague 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”, debido a que en mecánica cuántica es imposible

controlar con certeza, es decir, con probabilidad 1, la reacción del sistema ante el instrumento de medida, lo cual es conocido como principio de incertidumbre.

Más tarde, en 1952 D. Bohm introduce una nueva interpretación de la mecánica cuántica, la cual buscaba entender la teoría en términos de variables “ocultas” [28]. Con estas variables era posible determinar, al menos en principio, de manera precisa el resultado de cada proceso individual de medida. Además, señalaba que la mecánica cuántica puede ser generalizada, al considerar que las perturbaciones en el proceso de medida podrían ser eliminadas. Según esto, el principio de incertidumbre podría no ser válido.

1964 resultó ser un año esencial para aclarar las interpretaciones de la mecánica cuántica, ya que J. Bell [29] propuso una prueba experimental para determinar si los argumentos de EPR eran válidos. El resultado es conocido como la “desigualdad de Bell” (ver apéndice A), que es completamente general y no depende de una teoría física en particular; Mediante esta fue posible demostrar que, al considerar estados entrelazados no se satisface la desigualdad de Bell, lo que está en acuerdo con las predicciones de la mecánica cuántica, con el argumento de Bohr, y en contradicción con las ideas de la paradoja EPR. Es el requisito de localidad el que crea la dificultad esencial, esto es, 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. De esta forma, no existe una teoría física sobre variables ocultas que reproduzca todas las predicciones de la mecánica cuántica.

4.3.2. Definición

Para un sistema compuesto de dos partes, comúnmente denominadas Alice (A) y Bob (B), el estado total del sistema cuántico viene dado por

$$|\psi\rangle = |a\rangle \otimes |b\rangle, \quad (4.3.1)$$

donde los estados $|a\rangle$ y $|b\rangle$ son elementos de los espacios de Hilbert locales \mathcal{H}_A y \mathcal{H}_B , respectivamente.

Estados de la forma (4.3.1) no están entrelazados y son llamados *estados separables*, sin embargo, no todos los estados son separables, ya que la mecánica cuántica

también permite superposiciones que no son necesariamente productos:

$$|\phi\rangle = \frac{1}{N}(|a_1\rangle \otimes |b_1\rangle + |a_2\rangle \otimes |b_2\rangle), \quad (4.3.2)$$

donde N es tal que $\langle\phi|\phi\rangle = 1$. Si $|\phi\rangle$ no se puede escribir como un producto, es decir, $|\phi\rangle \neq |a\rangle \otimes |b\rangle$, entonces es llamado *estado entrelazado*.

Un estado mixto es separable si puede ser escrito como [30]

$$\rho = \sum_i p_i |a_i\rangle\langle a_i| \otimes |b_i\rangle\langle b_i|. \quad (4.3.3)$$

Los estados puros $|a_i\rangle$ y $|b_i\rangle$ son elementos de los espacios de Hilbert locales \mathcal{H}_A y \mathcal{H}_B , y $p_i \geq 0$ son probabilidades tal que $\sum_i p_i = 1$. Si el estado no puede ser escrito en esta forma, es llamado entrelazado.

4.4. Operaciones Cuánticas

El formalismo de las operaciones cuánticas permite describir la dinámica de los sistemas cuánticos en una gran variedad de escenarios, como por ejemplo, los sistemas cuánticos abiertos, los cuales se encuentran fuertemente acoplados con su medio ambiente [5]. En el formalismo de las operaciones cuánticas, el estado del sistema se describe mediante el operador densidad ρ , el cual transforma de la siguiente forma

$$\rho' = \Lambda(\rho). \quad (4.4.1)$$

El mapa Λ es un operador lineal que actúa sobre operadores⁵ [31], describe la dinámica del cambio de estado que ocurre como resultado de algún proceso físico y se le denomina *operación cuántica* [5].

Algunos ejemplos de operaciones cuánticas son: las transformaciones unitarias, $\Lambda(\rho) = U\rho U^\dagger$ y las mediciones cuánticas $\Lambda_m(\rho) = M_m\rho M_m^\dagger$.

⁵Este ente matemático a veces es llamado *superoperador*.

4.4.1. Operaciones Locales

Considérese el escenario donde Alice y Bob comparten un estado cuántico global ρ_{AB} de dos partículas y tienen permitido cualquier operación cuántica local, las que se denotarán $\mathcal{A} \otimes I_B$ y $I_A \otimes \mathcal{B}$, respectivamente. En general, la operación cuántica local puede ser cualquier transformación local, incluyendo una medición promedio sobre todos los posibles resultados [32]. Es importante resaltar que la aplicación de una operación cuántica local por una de las partes, no es necesariamente conocida por su contraparte con quien comparte el estado ρ_{AB} .

Además, es posible descomponer una operación cuántica local arbitraria en término de procesos más simples [24]. Estos son:

- **Transformación local unitaria:**

$$\rho_{AB} \rightarrow \rho'_{AB} = (U_A \otimes I_B)\rho(U_A^\dagger \otimes I_B), \quad (4.4.2)$$

donde U_A es una transformación unitaria que actúa sobre el subsistema de Alice. Análogamente, para el caso del subsistema de Bob se tiene el operador $I_A \otimes U_B$ actuando sobre ρ_{AB} .

- **Mediciones locales tipo von Neumann:**

Alice mide alguna cantidad sobre su subsistema, proceso que está simulado por la aplicación de un proyector $P_k = P_{AB}^k \otimes I_B$ local sobre el operador densidad ρ_{AB} . El resultado de la medida se obtiene con probabilidad p_k y proyecta el sistema total al estado $\rho_{AB}^k = P^k \rho_{AB} = (P_{AB}^k \otimes I_B)\rho_{AB}$. Los proyectores $\{P_k\}$ son mutuamente ortogonales.

- **Adjuntar una ancilla**

Esta operación consiste en aumentar la dimensión del espacio de Hilbert mediante la inclusión de un nuevo sistema físico. El estado de este sistema no se encuentra correlacionado con el sistema total, sin embargo se acopla a uno de los observadores.

$$\rho_{AB} \rightarrow \rho_{ABC} = \rho_{AB} \otimes \rho_C. \quad (4.4.3)$$

- **Eliminación de la ancilla**

El sistema auxiliar acoplado al sistema total puede ser eliminado trazando sobre él, es decir

$$\rho_{ABC} \rightarrow \rho'_{AB} = \text{Tr}_C(\rho_{ABC}). \quad (4.4.4)$$

La comunicación clásica posibilita que algunas operaciones cuánticas locales dependan del resultado de otras, lo que origina la existencia de transformaciones locales que no forman parte del conjunto de operaciones cuánticas locales. A pesar de esto, dichas transformaciones pueden ser escritas en términos de los cuatros procesos (anteriormente listados) junto a un nuevo proceso.

Supóngase que Alice y Bob comparten un sistema compuesto descrito en el espacio de Hilbert $\mathcal{H}_A \otimes \mathcal{H}_B$. Estos subespacios pueden estar asociados, por ejemplo, a dos partículas con idénticas características, una en poder de Alice y otra en poder de Bob. Así, el estado de ambos subsistemas está descrito por el operador densidad $\rho_{AB}^{(1)}$. Además, supóngase que los observadores comparten un segundo par de partículas en el estado $\rho_{AB}^{(2)}$. Alice, con una probabilidad q_1 elimina una de las partículas en su poder, de manera que termina con el estado $\rho_{AB}^{(1)}$ y comunica su intención a Bob, quien elimina la partícula correspondiente. Posterior a este proceso, los observadores finalizan con uno de los dos posibles estados, esto es

$$\rho = \rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} \rightarrow \left\{ q_1, \rho_{AB}^{(1)} \otimes I^{(2)}; 1 - q_1, I^{(1)} \otimes \rho_{AB}^{(2)} \right\}. \quad (4.4.5)$$

Nótese que si Alice no comunica su elección de partícula a eliminar y borra el registro de las elecciones anteriores, el estado final será

$$\rho = \rho_{AB}^{(1)} \otimes \rho_{AB}^{(2)} \rightarrow \rho' = q_1 \rho_{AB}^{(1)} \otimes I^{(2)} + (1 - q_1) I^{(1)} \otimes \rho_{AB}^{(2)}. \quad (4.4.6)$$

El obtener alguno de los estados (4.4.5) o (4.4.6) depende únicamente de la información disponible a los observadores. Luego, se tiene un nuevo proceso fundamental,

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

$$\{q_k, \rho_k\} \rightarrow \rho' = \sum_k q_k \rho_k, \quad (4.4.7)$$

donde $\sum_k q_k \rho_k$ corresponde a cualquier conjunto representado por ρ' .

4.4.2. Operaciones Locales y Comunicación Clásica (LOCC)

La idea detrás de la definición de estado separable presentada en la sección 4.3.2 es la siguiente: supóngase que Alice y Bob son capaces de producir cualquier estado cuántico de forma local. Además, ellos tienen acceso a un canal de comunicación clásica, tal como un teléfono. Entonces, Alice y Bob pueden producir cualquier estado separable de la forma (4.3.3) mediante el siguiente procedimiento: Alice prepara el estado $|a_i\rangle$ con probabilidad p_i y le hace saber a Bob qué estado preparó. Dependiendo de esta información, Bob prepara el correspondiente estado $|b_i\rangle$; Cabe señalar que de esta forma no es posible crear estados entrelazados.

El proceso de creación de estados separables presentado previamente, pertenece a la clase de *Operaciones Locales y Comunicación Clásica* o inglés *Local Operations and Classical Communication* (LOCC), introducido primeramente [13] en [33]. Además, si Alice y Bob están limitados solo a comunicación clásica, entonces esta clase de operaciones describe el procedimiento más general que ellos pueden aplicar en teoría cuántica. La descripción matemática general de estas operaciones es exigente [34], pero la idea es simple y se explicará a continuación.

Para dos partes, Alice y Bob, una operación cuántica Λ_{LOCC} pertenece a la clase de LOCC si puede ser descompuesta en los siguientes pasos:

1. Una de las partes, por ejemplo Alice, realiza una medición local sobre su subsistema.
2. El resultado de la medición es comunicado *clásicamente* a la otra parte, en este caso Bob.
3. Dependiendo de la información recibida, Bob realiza una medición local sobre su subsistema.
4. El resultado de la medición de Bob es comunicado clásicamente a Alice.
5. Dependiendo de la información recibida, Alice realiza una medición local sobre su subsistema, y el proceso comienza otra vez en el paso 2.

La clase de LOCC juega un papel importante en teoría de la información cuántica,

especialmente cuando se estudia entrelazamiento [13]. Nótese que cualquier estado separable puede ser creado con LOCC, sin embargo las LOCC no pueden ser usadas para crear estados entrelazados [35].

4.5. Cuantificación del entrelazamiento

El entrelazamiento es un fenómeno cuántico por excelencia y desempeña un papel central en información cuántica. Hace posible procesos como teleportación, codificación superdensa y subyace al incremento de la velocidad en algoritmos cuánticos. Por esta razón es útil pensar el entrelazamiento como un recurso, tanto para computación cuántica como para procesamiento de información cuántica. Los sistemas entrelazados, especialmente cuando se comparten, son en gran medida un recurso para las comunicaciones cuánticas. Y como recurso, es importante poder cuantificar la cantidad de entrelazamiento asociado con cualquier estado dado [7].

Un posible criterio para medir entrelazamiento pudo haber sido la desigualdad de Bell [29], pero existen estados parcialmente entrelazados que no la satisfacen [30] y por esto, dicha desigualdad no puede ser utilizada como medida.

Muchos trabajos han estado dedicados a la búsqueda de medidas de entrelazamiento y en particular, enfocados en estados mixtos de un sistema bipartito [33, 36, 37]. Y una de las medidas más populares es el entrelazamiento de formación, el cual cuantifica los recursos necesarios para crear un estado entrelazado dado [33].

4.5.1. Entropía de Entrelazamiento

Para un estado puro $|\psi_{AB}\rangle$ distribuido entre dos partes, el entrelazamiento es usualmente cuantificado por la *entropía de entrelazamiento*, que no es más que la entropía de von Neumann del operador densidad reducido $\rho_A = \text{Tr}_B(|\psi_{AB}\rangle\langle\psi_{AB}|)$,

$$E(|\phi_{AB}\rangle) = S(\rho_A) = - \sum_i \lambda_i \log_2 \lambda_i, \quad (4.5.1)$$

donde λ_i son autovalores de ρ_A . Se obtiene el mismo resultado si se utiliza el operador densidad reducido $\rho_B = \text{Tr}_A(|\psi_{AB}\rangle\langle\psi_{AB}|)$, esto es $E(|\phi_{AB}\rangle) = S(\rho_B)$.

4.5.2. Criterios para una medida de entrelazamiento

Para estados mixtos no existe una única cuantificación del entrelazamiento, pero una posible medida E debiese satisfacer las condiciones [39]:

- i) Para un sistema bipartito $E(\rho)$ debe ser un mapeo desde operadores densidad a números reales positivos.
- ii) Debe ser cero, si el estado es separable.
- iii) La medida no debe en promedio aumentar bajo LOCC.
- iv) Para estados puros la medida de entrelazamiento se debe reducir a la entropía de entrelazamiento (4.5.1). Para estados maximalmente entrelazados la medida se reduce a $\log_2 d$.

Sin embargo, algunos autores [39, 40] exigen otras propiedades que debe cumplir E :

- v) Continuidad: El entrelazamiento debe converger a cero; en el límite cuando la distancia de dos operadores densidad distintos tiende a cero, es decir, $E(\rho) - E(\sigma) \rightarrow 0$ para $\|\rho - \sigma\| \rightarrow 0$.
- vi) Aditividad: Un número n de copias idénticas del estado ρ debe contener n veces el entrelazamiento de una copia, es decir, $E(\rho^{\otimes n}) = nE(\rho)$.
- vii) 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, $E(\rho \otimes \sigma) \leq E(\rho) + E(\sigma)$.
- viii) 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 $0 < \lambda < 1$.

4.5.3. Medidas de entrelazamiento para estados mixtos

Para una estado mixto ρ_{AB} se consideran dos clases principales de medidas de entrelazamiento [13]:

- medidas de techo convexo (*convex roof measures*) y

- medidas basadas en la distancia⁶.

Cualquier medida de entrelazamiento E que se define sobre estados puros puede ser extendida a estados mixtos mediante la construcción de techo convexo (*convex roof*) [13, 41]

$$E(\rho) = \min_{\{p_i, |\psi_i\rangle\}} \left\{ \sum_i p_i E(|\psi_i\rangle) \right\}, \quad (4.5.2)$$

donde el mínimo es tomado sobre todas las descomposiciones $\{p_i, |\psi_i\rangle\}$ del operador densidad ρ dado con probabilidad p_i no negativas, es decir, $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$.

4.5.4. Entrelazamiento de Formación

Para sistemas bipartitos, el *entrelazamiento de formación* E_f definido en [33] es una de las más populares y frecuentemente usadas medidas de techo convexo [13]. Para estados puros se define como la entropía de entrelazamiento (4.5.1) y la extensión a estados mixtos se realiza mediante la construcción de techo convexo (4.5.2), esto es

$$E_f(\rho_{AB}) = \min_{\{p_i, |\psi_i\rangle\}} \left\{ \sum_i p_i E(|\psi_i\rangle) \right\}, \quad (4.5.3)$$

donde $E(|\psi_i\rangle)$ corresponde a la entropía de entrelazamiento (4.5.1).

Aunque en general, es difícil de evaluar analíticamente el mínimo en (4.5.3), Wootters presentó una expresión explícita para el entrelazamiento de formación de estados mixtos arbitrarios de dos qubits [42]. Así, para cualquier estado ρ_{AB} de este tipo, el entrelazamiento de formación E_f viene dado por

$$E_f(\rho_{AB}) = h\left(\frac{1 + \sqrt{1 - C^2(\rho_{AB})}}{2}\right), \quad (4.5.4)$$

donde $E_f(\rho_{AB})$ es monótonamente creciente y oscila entre 0 y 1, h es la *entropía binaria* definida como $h(x) = -x \log_2 x - (1 - x) \log_2(1 - x)$, y $C(\rho_{AB})$ es la

⁶Se menciona solo por completitud, ya que en este trabajo se utiliza una medida de techo convexo para cuantificar el entrelazamiento. En particular, se hace uso de la concurrencia; cantidad definida en el cálculo del Entrelazamiento de Formación.

llamada *conurrencia*:

$$C(\rho_{AB}) = \max \{0, \lambda_1 - \lambda_2 - \lambda_3 - \lambda_4\}, \quad (4.5.5)$$

con λ_i los autovalores (no negativos) en orden decreciente de la matriz hermítica $R \equiv \sqrt{\sqrt{\rho}\rho\sqrt{\rho}}$. De forma alternativa, se puede decir que los λ_i son las raíces cuadradas de los autovalores de la matriz antihermítica $\rho\tilde{\rho}$ con,

$$\tilde{\rho}_{AB} = (\sigma_y \otimes \sigma_y) \rho_{AB}^* (\sigma_y \otimes \sigma_y). \quad (4.5.6)$$

En el caso de sistemas puros la conurrencia se reduce a una expresión más simple:

$$C(\psi) = \left| \langle \psi | \tilde{\psi} \rangle \right|, \quad (4.5.7)$$

donde $|\tilde{\psi}\rangle = \sigma_y |\psi^*\rangle$.

Se debe señalar que el entrelazamiento de formación satisface los criterios para una medida de entrelazamiento adecuada, y además, dado que la relación entre el entrelazamiento de formación y la conurrencia es monótonamente creciente, se puede considerar a esta última como una buena medida de entrelazamiento [42].

4.5.5. Entrelazamiento Residual o *Three-tangle*

El *entrelazamiento residual* o también conocido como *three-tangle* es una medida de entrelazamiento para sistemas tripartitos introducida en [45].

Para estados puros (de sistemas compuestos de tres qubits) de la forma

$$|\psi_{ABC}\rangle = \sum_{ijk} a_{ijk} |ijk\rangle, \quad (4.5.8)$$

con $a_{ijk} \in \mathbb{C}$ y $\{|ijk\rangle\}$ la base estándar, donde cada índice toma los valores 0 y 1, se define el *three-tangle* τ_{ABC} como

$$\tau_{ABC} = 2 \left| \sum a_{ijk} a_{i'j'm} a_{npk'} a_{n'p'm'} \epsilon_{ii'} \epsilon_{jj'} \epsilon_{kk'} \epsilon_{mm'} \epsilon_{nn'} \epsilon_{pp'} \right|, \quad (4.5.9)$$

donde la suma es sobre todos los índices y

$$\begin{aligned}\epsilon_{00} &= \epsilon_{11} = 0, \\ \epsilon_{01} &= -\epsilon_{10} = 1.\end{aligned}$$

El *three-tangle* representa una propiedad colectiva de los tres qubits. Esto es, el entrelazamiento del sistema se puede manifestar de distantes maneras: el sistema A entrelazado con BC (visto como un solo sistema), el sistema A entrelazado con B , el sistema A entrelazado con C o un entrelazamiento global ABC . Esto se puede expresar como [45]

$$C_{A(BC)}^2 = C_{AB}^2 + C_{AC}^2 + \tau_{ABC}, \quad (4.5.10)$$

donde C es la concurrencia definida en la sección 4.5.4.

4.6. Clasificación de estados cuánticos

Si bien en la sección 4.3.2 se presentó la definición de un estado separable y un estado entrelazado, en esta sección se hará una clasificación más detallada de estados cuánticos, la cual está basado en [43].

Considérese un sistema cuántico compuesto de N subsistemas físicamente distinguibles A, B, C, \dots , cuyo operador densidad es $\rho_{ABC\dots}$, y el operador densidad del i -ésimo sistema se obtiene al trazar parcialmente sobre todos los otros subsistemas.

4.6.1. Estado producto

Se dice que $\rho_{ABC\dots}$ es un *estado producto* si es posible escribirlo como el producto tensorial de los respectivos operadores densidad reducidos, esto es,

$$\rho_{ABC\dots} = \rho_A \otimes \rho_B \otimes \rho_C \otimes \dots \quad (4.6.1)$$

Los estados producto no presentan correlaciones. Nótese que la mezcla de dos estados producto pertenece al conjunto de los estados separables.

4.6.2. Estados separables

Un operador densidad representa un *estado separable* si puede escribirse como mezcla de estados productos [30],

$$\rho_{ABC\dots} = \sum_i p_i \rho_A^i \otimes \rho_B^i \otimes \rho_C^i \otimes \dots \quad (4.6.2)$$

donde $\rho_A^i, \rho_B^i, \rho_C^i, \dots$ corresponden a los operadores densidad de los subsistemas A, B, C, \dots respectivamente y $\sum_i p_i = 1$.

Estos estados se caracterizan por satisfacer la desigualdad de Bell (A0.8). Además, como se hizo mención en la sección 4.4.2, estos estados pueden prepararse utilizando LOCC.

4.6.3. Estado clásico

Un estado clásico tiene la particularidad de poseer solo correlaciones clásicas [44]. Se construye como una mezcla de estados puros no entrelazados, localmente ortogonales y es de la forma

$$\begin{aligned} \rho_{ABC\dots} &= \sum_{k_1, \dots, k_N} p_{k_1 \dots k_N} |k_1\rangle\langle k_1| \otimes \dots \otimes |k_N\rangle\langle k_N| \\ &= \sum_{\vec{k}} p_{\vec{k}} |\vec{k}\rangle\langle \vec{k}|, \end{aligned} \quad (4.6.3)$$

donde los estados $|\vec{k}\rangle$ denotan un producto tensorial de N estados $|k_i\rangle$ que definen una base ortogonal en cada subsistema. Dicho de otra manera, los autoestados del operador densidad que describe un estado clásico son factorizados y además localmente ortogonales.

La mezcla de estados clásicos conduce, en general, a un estado separable. Y cuando dos estados son clásicos y poseen los mismos autovalores, la mezcla de ellos sigue siendo clásica.

Dado que las correlaciones cuánticas generalmente no son simétricas, es posible definir *estados semi-clásicos*, los cuales son clásicos tan solo en una de sus partes.

4.6.4. Estados entrelazados

Como contraparte a los estados separables que no presentan entrelazamiento, pero sí correlaciones clásicas, existen los llamados *estados entrelazados*. Esto es, un operador densidad representa un estado entrelazado si no representa un estado separable. Debe notarse que la mezcla de estados entrelazados puede dar como resultado un estado separable.

4.6.4.1. Estados de Bell

Un estado de Bell o también conocido como par EPR⁷, es un estado que está maximalmente entrelazado entre dos sistemas. Estos estados forman una base ortogonal denominada base de Bell.

$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), \quad (4.6.4a)$$

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle). \quad (4.6.4b)$$

4.6.4.2. Estados W

$$|W_1\rangle = \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}, \quad (4.6.5)$$

$$|W_2\rangle = \frac{|101\rangle + |110\rangle + |011\rangle}{\sqrt{3}}. \quad (4.6.6)$$

4.6.4.3. Estados Greenberger-Horne-Zeilinger (GHZ)

$$|\text{GHZ}_\pm\rangle = \frac{|000\rangle \pm |111\rangle}{\sqrt{2}}. \quad (4.6.7)$$

⁷Einstein, Podolsky y Rosen.

4.7. Extracción de Entrelazamiento Determinista (DEE)

En el año 2019 se propuso un esquema de *Extracción de Entrelazamiento Determinista* [46] (o DEE⁸, por sus siglas en inglés) por medio de un proceso de reducción que involucra mediciones locales tipo von Neumann (ver sección 4.4.1): con una base adecuada se puede mapear un estado de tres qubits en un estado puro de dos qubits con la misma cantidad de entrelazamiento de formación, resultando en un mejoramiento del entrelazamiento del estado bipartito con respecto al estado mixto inicial.

Se considera un estado puro de tres qubits $|\psi\rangle$ con coeficientes reales,

$$|\psi\rangle = \sum_{p,q,r,s=0}^1 c_{pqr} |pqr\rangle, \quad c_{pqr} = c_{pqr}^*, \quad \sum_{p,q,r=0}^1 c_{pqr}^2 = 1.$$

caracterizado por un *three-tangle* τ y concurrencias C_{ij} , $i, j, k = 1, 2, 3$, las cuales describen los correspondientes estados reducidos $\rho_{ij} = \text{Tr}_k(|\psi\rangle\langle\psi|)$. Se realiza una medición local sobre el primer qubit, y se tienen los dos resultados siguientes:

1. Si el qubit se proyecta sobre el estado

$$|\theta, \phi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad (4.7.1)$$

donde θ y ϕ son los ángulos en la esfera de Bloch y $\{|0\rangle, |1\rangle\}$ son los autoestados del operador de Pauli σ_z , el estado puro bipartito resultante es

$$|\psi_{\theta,\phi}\rangle = \frac{1}{\sqrt{p_{\theta,\phi}}} \langle\theta, \phi|\psi\rangle, \quad (4.7.2)$$

y se obtiene con una probabilidad de $p_{\theta,\phi} = \text{Tr}(\langle\theta, \phi|\psi\rangle \langle\psi|\theta, \phi\rangle)$.

2. Si el qubit se proyecta sobre el estado ortogonal $|\theta + \pi, \phi\rangle$, entonces el estado puro bipartito resultante es

$$|\psi_{\theta+\pi,\phi}\rangle = \frac{1}{\sqrt{p_{\theta+\pi,\phi}}} \langle\theta + \pi, \phi|\psi\rangle, \quad (4.7.3)$$

⁸*Deterministic Entanglement Extraction.*

y se obtiene con una probabilidad $p_{\theta+\pi,\phi} = 1 - p_{\theta,\phi}$.

El escenario determinista corresponde al caso cuando ambos resultados, $|\psi_{\theta,\phi}\rangle$ y $|\psi_{\theta+\pi,\phi}\rangle$, tienen el mismo valor de concurrencia⁹ C_d . Además, esta está acotada por

$$C_{23} \leq C_d \leq \sqrt{\tau + C_{23}^2}. \quad (4.7.4)$$

Cuando el proceso de Extracción de Entrelazamiento Determinista es óptimo, la concurrencia de los estados resultantes es

$$C_d = \sqrt{\tau + C_{23}^2}. \quad (4.7.5)$$

4.7.1. Concurrencia, *three-tangle* y probabilidad

Para obtener los resultados precedentes, en el trabajo [46] introducen las siguientes definiciones

$$\mathbf{n} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix} = \begin{pmatrix} \sin \theta \cos \phi \\ \sin \theta \sin \phi \\ \cos \theta \end{pmatrix}, \quad (4.7.6)$$

$$\mathbf{X} = \begin{pmatrix} X_x \\ X_y \\ X_z \end{pmatrix} = \begin{pmatrix} \langle \psi | I \otimes \sigma_y \otimes \sigma_y | \psi \rangle \\ \langle \psi | \sigma_x \otimes \sigma_y \otimes \sigma_y | \psi \rangle \\ \langle \psi | \sigma_z \otimes \sigma_y \otimes \sigma_y | \psi \rangle \end{pmatrix}, \quad (4.7.7)$$

$$\mathbf{Y} = \begin{pmatrix} Y_x \\ Y_y \\ Y_z \end{pmatrix} = \begin{pmatrix} \langle \psi | \sigma_x \otimes I \otimes I | \psi \rangle \\ \langle \psi | \sigma_y \otimes I \otimes I | \psi \rangle \\ \langle \psi | \sigma_z \otimes I \otimes I | \psi \rangle \end{pmatrix}, \quad (4.7.8)$$

$$\mathbf{M}_{\pm} = \begin{pmatrix} n_x^2 + n_z^2 & \pm n_x + in_y n_z & \pm n_z - in_x n_y \\ \pm n_x - in_y n_z & 1 - n_z^2 & n_x n_z \mp in_y \\ \pm n_z + in_x n_y & n_x n_z \pm in_y & 1 - n_x^2 \end{pmatrix}. \quad (4.7.9)$$

⁹Ver Apéndice B para más detalles.

Con estas definiciones se pueden escribir la probabilidad y concurrencia asociada a cada estado resultante luego de la medición local,

$$p_{\theta,\phi} = p_{+\mathbf{n}} = \frac{1}{2}(1 + \mathbf{n}^\dagger \mathbf{Y}), \quad (4.7.10)$$

$$p_{\theta+\pi,\phi} = p_{-\mathbf{n}} = \frac{1}{2}(1 - \mathbf{n}^\dagger \mathbf{Y}), \quad (4.7.11)$$

$$|C_{\theta,\phi}|^2 = |C_+|^2 = \frac{1}{4p_{+\mathbf{n}}^2} \mathbf{X}^\dagger \mathbf{M}_+ \mathbf{X}, \quad (4.7.12)$$

$$|C_{\theta+\pi,\phi}|^2 = |C_-|^2 = \frac{1}{4p_{-\mathbf{n}}^2} \mathbf{X}^\dagger \mathbf{M}_- \mathbf{X}, \quad (4.7.13)$$

además, también se puede escribir la concurrencia de un par de qubits antes la medición local y el *three-tangle* del estado tripartito inicial, esto es

$$C_{23} = \frac{1}{\sqrt{2}} \sqrt{X_x^2 + X_y^2 + X_z^2 - |X_y^2 + X_z^2 - X_x^2|}, \quad (4.7.14)$$

$$\tau = |X_y^2 + X_z^2 - X_x^2|. \quad (4.7.15)$$

En el caso que el estado tripartito considerado solo tenga coeficientes reales, $Y_y = 0$ [46].



4.8. Método Procusteano

El *método Procusteano*¹⁰ o *filtrado local*, fue presentado en [36] el año 1996 y permite transformar un estado parcialmente entrelazado en uno maximalmente entrelazado [47].

Supónganse dos partículas parcialmente entrelazadas, de las cuales una está en posesión de Alice (A) y la otra de Bob (B), en el estado¹¹

$$|\psi\rangle = \alpha |0\rangle_A |0\rangle_B + \sqrt{1 - \alpha^2} |1\rangle_A |1\rangle_B, \quad \alpha \in \mathbb{R}. \quad (4.8.1)$$

Para implementar este método, el sistema A (o B) se acopla a un sistema auxiliar

¹⁰*Procrustean Method* en inglés.

¹¹El estado en consideración es un caso especial de una descomposición de Schmidt [47].

a en un estado conocido mediante una operación unitaria conjunta U_{Aa} , tal que

$$\begin{aligned} U_{Aa} |0\rangle_A |0\rangle_a &= \epsilon_1 |0\rangle_A |0\rangle_a + \epsilon_2 |0\rangle_A |1\rangle_a, \\ U_{Aa} |1\rangle_A |0\rangle_a &= |1\rangle_A |0\rangle_a, \end{aligned} \quad (4.8.2)$$

con $\epsilon_i \in \mathbb{R}$ y $\epsilon_1^2 + \epsilon_2^2 = 1$, y

$$\begin{aligned} |\psi'\rangle &= U_{Aa} |\psi\rangle |0\rangle_a \\ &= \left(\epsilon_1 \alpha |0\rangle_A |0\rangle_B + \sqrt{1 - \alpha^2} |1\rangle_A |1\rangle_B \right) |0\rangle_a + \epsilon_2 \alpha |0\rangle_A |0\rangle_B |1\rangle_a \\ &= \sqrt{1 - \alpha^2 (1 - \epsilon_1^2)} \frac{\left(\epsilon_1 \alpha |0\rangle_A |0\rangle_B + \sqrt{1 - \alpha^2} |1\rangle_A |1\rangle_B \right)}{\sqrt{1 - \alpha^2 (1 - \epsilon_1^2)}} |0\rangle_a + \epsilon_2 \alpha |0\rangle_A |0\rangle_B |1\rangle_a. \end{aligned} \quad (4.8.3)$$

Al escoger la operación unitaria de tal forma que $\epsilon_1 = \sqrt{1 - \alpha^2}/\alpha$, se obtiene

$$|\psi'\rangle = \sqrt{2(1 - \alpha^2)} \frac{|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B}{\sqrt{2}} |0\rangle_a + \epsilon_2 \alpha |0\rangle_A |0\rangle_B |1\rangle_a. \quad (4.8.4)$$

Luego, al realizar una medición en la base $\{|0\rangle, |1\rangle\}$ del sistema auxiliar, el estado $|\psi\rangle$ inicial se transforma en un estado de Bell con una probabilidad de éxito

$$p_{\text{Bell}} = 2(1 - \alpha^2), \quad (4.8.5)$$

o se pierde todo el entrelazamiento inicial, con una probabilidad $1 - p_{\text{Bell}}$ de que esto suceda.

Capítulo 5

Generación probabilística de estados de Bell

5.1. Probabilidad de éxito Método Procusteano

Utilizando el método Procusteano, la probabilidad de éxito p_{Bell} de transformar un estado de la forma

$$|\psi'\rangle = \alpha |00\rangle + \sqrt{1 - \alpha^2} |11\rangle, \quad \alpha \in \mathbb{R}, \quad (5.1.1)$$

a un estado maximalmente entrelazado, viene dada por (4.8.5) y es

$$p_{\text{Bell}} = 2(1 - \alpha^2).$$

La concurrencia $C(\psi') = \left| \langle \psi' | \tilde{\psi}' \rangle \right|$ del estado (5.1.1) viene dada por

$$C(\psi') = 2\alpha\sqrt{1 - \alpha^2}. \quad (5.1.2)$$

A continuación se reescribirá la probabilidad p_{Bell} en términos de la concurrencia, para ello se despeja α^2 de la expresión (5.1.2) y se obtiene

$$\alpha_{\pm}^2 = \frac{1 \pm \sqrt{1 - C^2(\psi')}}{2}. \quad (5.1.3)$$

En el proceso se ha tenido que elevar al cuadrado la expresión (5.1.2), lo que ha

añadido una solución que se descartará posteriormente.

Al introducir (5.1.3) en p_{Bell} se obtiene

$$p_{\text{Bell}}^{\pm} = 1 \mp \sqrt{1 - C^2(\psi')}.$$

Como la probabilidad debe estar en el rango de 0 a 1, la solución a descartar es α_-^2 , así, la probabilidad de éxito p_{Bell} para generar un estado de Bell utilizando el Método Procusteano en términos de la concurrencia es dada por

$$p_{\text{Bell}} = 1 - \sqrt{1 - C^2(\psi')}. \quad (5.1.4)$$

5.2. Desarrollo de Estrategias

Para el desarrollo de las estrategias se consideran estados tripartitos puros con coeficientes reales,

$$|\psi\rangle = \sum_{p,q,r,s=0}^1 c_{pqr} |pqr\rangle, \quad c_{pqr} = c_{pqr}^*, \quad \sum_{p,q,r=0}^1 c_{pqr}^2 = 1. \quad (5.2.1)$$

5.3. Estrategia 1

Esta estrategia para generar estados de Bell consiste en aplicar el esquema de Extracción de Entrelazamiento Determinista sobre el estado (5.2.1), obteniendo dos estados puros con igual concurrencia C_d y cuyo valor máximo viene dado por la expresión (4.7.5), esto es,

$$C_d = \sqrt{\tau + C^2(\rho_{23})},$$

donde la concurrencia $C(\rho_{23}) = C_{23}$ y *three-tangle* τ se obtienen de (4.7.14) y (4.7.15), respectivamente.

Posteriormente, sobre los estados de salida obtenidos a través del proceso de Extracción de Entrelazamiento Determinista se aplica el método Procusteano antes descrito. De esta forma, de acuerdo a (5.1.4) la máxima probabilidad de

éxito de esta estrategia es

$$p_{\text{éxito}}^{(1)} = 1 - \sqrt{1 - C_d^2} = 1 - \sqrt{1 - (\tau + C_{23}^2)}. \quad (5.3.1)$$

5.4. Estrategia 2

La estrategia para generar estados de Bell que se desarrolla en esta sección consiste en medir sobre un qubit del estado tripartito inicial (5.2.1), un observable con estados propios $\{|\theta, \phi\rangle, |\theta + \pi, \phi\rangle\}$, para luego buscar el conjunto de ángulos $\{\theta_s, \phi_s\}$ en el cual la concurrencia de uno de los resultados de medida sea 1, y sobre la salida ortogonal aplicar el método Procusteano que permita transformarlo en un estado maximalmente entrelazado. Así, independiente del resultado de medida, el estado resultante es maximalmente entrelazado.

Se realiza una medición local sobre el primer qubit de (5.2.1) y se obtienen los dos resultados siguientes:

1. Si el estado tripartito (5.2.1) se proyecta sobre el estado

$$|\theta, \phi\rangle = \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle, \quad (5.4.1)$$

donde θ y ϕ son los ángulos en la esfera de Bloch y $\{|0\rangle, |1\rangle\}$ son los autoestados del operador de Pauli σ_z . El estado puro bipartito resultante es

$$|\psi_{\theta, \phi}\rangle = \frac{1}{\sqrt{p_{\theta, \phi}}} \langle \theta, \phi | \psi \rangle \quad (5.4.2)$$

con una probabilidad de

$$p_{\theta, \phi} = \text{Tr}(\langle \theta, \phi | \psi \rangle \langle \psi | \theta, \phi \rangle) \quad (5.4.3)$$

y su concurrencia es $C(|\psi_{\theta, \phi}\rangle)$.

2. Si el estado tripartito (5.2.1) se proyecta sobre el estado ortogonal

$$|\theta + \pi, \phi\rangle = \cos \frac{\theta + \pi}{2} |0\rangle + e^{i\phi} \sin \frac{\theta + \pi}{2} |1\rangle, \quad (5.4.4)$$

entonces el estado puro bipartito resultante es

$$|\psi_{\theta+\pi,\phi}\rangle = \frac{1}{\sqrt{p_{\theta+\pi,\phi}}} \langle \theta + \pi, \phi | \psi \rangle \quad (5.4.5)$$

y se obtiene con una probabilidad de $p_{\theta+\pi,\phi}$ y su concurrencia es $C(|\psi_{\theta+\pi,\phi}\rangle)$

A continuación, se busca el conjunto de ángulos $\{\theta_s, \phi_s\}$ para los cuales

$$C(|\psi_{\theta_s+\pi,\phi_s}\rangle) = 1. \quad (5.4.6)$$

Para el mismo conjunto de ángulos se tendrá

$$C(|\varphi_{\theta_s,\phi_s}\rangle) \neq 1. \quad (5.4.7)$$

Una vez determinado el conjunto de ángulos $\{\theta_s, \phi_s\}$ se aplica el método Procusteano sobre el estado $|\psi_{\theta_s,\phi_s}\rangle$ para transformarlo en uno maximalmente entrelazado, es decir, $C(|\psi_{\theta_s,\phi_s}\rangle) = 1$. De acuerdo a (5.1.4), la probabilidad de éxito de este proceso es

$$p_{\theta_s,\phi_s}^{\text{Bell}} = 1 - \sqrt{1 - C^2(|\psi_{\theta_s,\phi_s}\rangle)}. \quad (5.4.8)$$

De esta forma, la probabilidad de éxito de esta estrategia viene dada por

$$P_{\theta_s,\phi_s} = p_{\theta_s+\pi,\phi_s} + p_{\theta_s,\phi_s} p_{\theta_s,\phi_s}^{\text{Bell}}. \quad (5.4.9)$$

La razón de (5.4.9) se explica a continuación: Si \mathcal{A} es el evento de obtener el resultado de medida $|\psi_{\theta_s+\pi,\phi_s}\rangle$ con concurrencia $C(|\psi_{\theta_s+\pi,\phi_s}\rangle) = 1$, entonces la probabilidad de este evento es $p(\mathcal{A}) = p_{\theta_s+\pi,\phi_s}$. Así, el evento complementario \mathcal{A}^c es obtener el resultado de medida ortogonal, es decir, $|\psi_{\theta_s,\phi_s}\rangle$ con concurrencia $C(|\psi_{\theta_s,\phi_s}\rangle) \neq 1$, cuya probabilidad es $p(\mathcal{A}^c) = p_{\theta_s,\phi_s} = 1 - p_{\theta_s+\pi,\phi_s}$. Por otro lado, si \mathcal{B} es el evento de transformar el estado $|\psi_{\theta_s,\phi_s}\rangle$ en un estado de Bell mediante el Método Procusteano, entonces la probabilidad de dicho evento es $p(\mathcal{B}) = p_{\theta_s,\phi_s}^{\text{Bell}}$.

Se debe notar que, en principio, los eventos \mathcal{A} y \mathcal{B} son eventos estadísticamente independientes, por lo que la probabilidad de éxito de esta estrategia, es la suma de la probabilidad del evento \mathcal{A} y la probabilidad del evento $\mathcal{A}^c \cap \mathcal{B}$, esto es, la

probabilidad condicional.

Así, si del conjunto $\{\theta_s, \phi_s\}$ se escoge el conjunto de ángulos $\{\theta_{s^*}, \phi_{s^*}\}$ que maximice la probabilidad (5.4.9), la máxima probabilidad de éxito de esta estrategia será

$$p_{\text{éxito}}^{(2)} = P_{\theta_{s^*}, \phi_{s^*}} = \max_{\{\theta_s, \phi_s\}} \{P_{\theta_s, \phi_s}\} \quad (5.4.10)$$

A continuación, se realizará la maximización (5.4.10) para encontrar una expresión explícita para la máxima probabilidad de éxito de la Estrategia 2.

Se reescribe¹ (5.4.9) de la siguiente manera

$$\begin{aligned} P_{\theta_s, \phi_s} &= p_{\theta_s + \pi, \phi_s} + p_{\theta_s, \phi_s} p_{\theta_s, \phi_s}^{\text{Bell}} \\ &= p_{\theta_s + \pi, \phi_s} + p_{\theta_s, \phi_s} \left(1 - \sqrt{1 - C_{\theta_s, \phi_s}^2}\right) \\ &= p_{\theta_s + \pi, \phi_s} + p_{\theta_s, \phi_s} - p_{\theta_s, \phi_s} \sqrt{1 - C_{\theta_s, \phi_s}^2} \\ &= 1 - p_{\theta_s, \phi_s} \sqrt{1 - C_{\theta_s, \phi_s}^2} \\ &= 1 - \sqrt{p_{\theta_s, \phi_s}^2 - p_{\theta_s, \phi_s}^2 C_{\theta_s, \phi_s}^2} \end{aligned}$$

y con esto en mente, se escribe (5.4.10) como

$$\begin{aligned} p_{\text{éxito}}^{(2)} &= P_{\theta_{s^*}, \phi_{s^*}} \\ &= \max_{\{\theta_s, \phi_s\}} \{P_{\theta_s, \phi_s}\} \\ &= 1 - \min_{\{\theta_s, \phi_s\}} \left\{ \sqrt{p_{\theta_s, \phi_s}^2 - p_{\theta_s, \phi_s}^2 C_{\theta_s, \phi_s}^2} \right\} \end{aligned} \quad (5.4.11)$$

donde

$$\min_{\{\theta_s, \phi_s\}} \left\{ \sqrt{p_{\theta_s, \phi_s}^2 - p_{\theta_s, \phi_s}^2 C_{\theta_s, \phi_s}^2} \right\}$$

es equivalente a

$$\min_{\{\theta_s, \phi_s\}} \left\{ p_{\theta_s, \phi_s}^2 - p_{\theta_s, \phi_s}^2 C_{\theta_s, \phi_s}^2 \right\} \quad (5.4.12)$$

porque el término bajo raíz es una función monótonamente creciente.

¹Se hace $C(|\psi_{\theta_s, \phi_s}\rangle) = C_{\theta_s, \phi_s}$.

De esta forma, para encontrar una expresión explícita para $p_{\text{éxito}}^{(2)}$ se debe minimizar²

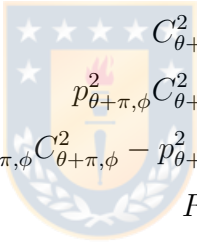
$$G_{\theta,\phi} = p_{\theta,\phi}^2 - p_{\theta,\phi}^2 C_{\theta,\phi}^2 \quad (5.4.13)$$

sujeta a las restricciones

$$\begin{aligned} C_{\theta+\pi,\phi} &= 1, \\ n_x^2 + n_y^2 + n_z^2 &= 1, \end{aligned}$$

donde p_{θ_s,ϕ_s} , C_{θ_s,ϕ_s}^2 y $C_{\theta_s+\pi,\phi_s}^2$ vienen dados por (4.7.10), (4.7.12) y (4.7.13), respectivamente. Y n_x , n_y y n_z son las componentes de (4.7.6).

Para evitar problemas con fracciones en la tarea de minimización, la restricción $C_{\theta+\pi,\phi} = 1$ se reescribe como



$$\begin{aligned} C_{\theta+\pi,\phi}^2 &= 1 \\ p_{\theta+\pi,\phi}^2 C_{\theta+\pi,\phi}^2 &= p_{\theta+\pi,\phi}^2 \\ p_{\theta+\pi,\phi}^2 C_{\theta+\pi,\phi}^2 - p_{\theta+\pi,\phi}^2 &= 0 \\ R_{\theta,\phi} &= 0, \end{aligned}$$

donde se ha definido

$$R_{\theta,\phi} = p_{\theta+\pi,\phi}^2 C_{\theta+\pi,\phi}^2 - p_{\theta+\pi,\phi}^2. \quad (5.4.14)$$

Se debe notar que $\mathbf{n} = \mathbf{n}(\theta, \phi)$, por lo que es posible escribir $\theta = \theta(\mathbf{n})$ y $\phi = \phi(\mathbf{n})$, de esta forma se puede expresar (5.4.13) y (5.4.14) como

$$G_{\mathbf{n}} = p_{\mathbf{n}}^2 - p_{\mathbf{n}}^2 C_{\mathbf{n}}^2, \quad (5.4.15)$$

$$R_{\mathbf{n}} = p_{-\mathbf{n}}^2 C_{-\mathbf{n}}^2 - p_{-\mathbf{n}}^2. \quad (5.4.16)$$

Por lo tanto, hay que resolver el problema de minimización

$$\min_{\{\mathbf{n}\}} \{G_{\mathbf{n}}\}, \quad (5.4.17)$$

²Se hace el cambio de notación: $\theta_s \rightarrow \theta$; $\phi_s \rightarrow \phi$.

sujeto a las restricciones

$$R_{\mathbf{n}} = 0, \quad (5.4.18)$$

$$n_x^2 + n_y^2 + n_z^2 = 1, \quad (5.4.19)$$

con

$$\mathbf{n} = \begin{pmatrix} n_x \\ n_y \\ n_z \end{pmatrix} = \begin{pmatrix} \sin \theta \cos \phi \\ \sin \theta \sin \phi \\ \cos \theta \end{pmatrix}, \quad (5.4.20)$$

$$\mathbf{X} = \begin{pmatrix} X_x \\ X_y \\ X_z \end{pmatrix} = \begin{pmatrix} \langle \psi | I \otimes \sigma_y \otimes \sigma_y | \psi \rangle \\ \langle \psi | \sigma_x \otimes \sigma_y \otimes \sigma_y | \psi \rangle \\ \langle \psi | \sigma_z \otimes \sigma_y \otimes \sigma_y | \psi \rangle \end{pmatrix}, \quad (5.4.21)$$

$$\mathbf{Y} = \begin{pmatrix} Y_x \\ Y_y \\ Y_z \end{pmatrix} = \begin{pmatrix} \langle \psi | \sigma_x \otimes I \otimes I | \psi \rangle \\ 0 \\ \langle \psi | \sigma_z \otimes I \otimes I | \psi \rangle \end{pmatrix}, \quad (5.4.22)$$

$$\mathbf{M}_{\pm} = \begin{pmatrix} n_x^2 + n_z^2 & \pm n_x + in_y n_z & \pm n_z - in_x n_y \\ \pm n_x - in_y n_z & 1 - n_z^2 & n_x n_z \mp in_y \\ \pm n_z + in_x n_y & n_x n_z \pm in_y & 1 - n_x^2 \end{pmatrix}. \quad (5.4.23)$$

y

$$p_{+\mathbf{n}} = \frac{1}{2}(1 + \mathbf{n}^\dagger \mathbf{Y}), \quad (5.4.24)$$

$$p_{-\mathbf{n}} = \frac{1}{2}(1 - \mathbf{n}^\dagger \mathbf{Y}), \quad (5.4.25)$$

$$C_+^2 = \frac{1}{4p_{+\mathbf{n}}^2} \mathbf{X}^\dagger \mathbf{M}_+ \mathbf{X}, \quad (5.4.26)$$

$$C_-^2 = \frac{1}{4p_{-\mathbf{n}}^2} \mathbf{X}^\dagger \mathbf{M}_- \mathbf{X}. \quad (5.4.27)$$

De esta forma, para realizar la minimización hay que utilizar multiplicadores de

Lagrange³ y resolver el sistema de ecuaciones

$$\begin{aligned}\nabla_{\mathbf{n}}[G_{\mathbf{n}} + \mu R_{\mathbf{n}} + \lambda(n_x^2 + n_y^2 + n_z^2 - 1)] &= 0, \\ R_{\mathbf{n}} &= 0, \\ n_x^2 + n_y^2 + n_z^2 &= 1.\end{aligned}\tag{5.4.28}$$

con $G_{\mathbf{n}}$ la función objetivo y $R_{\mathbf{n}} = 0$, $n_x^2 + n_y^2 + n_z^2 = 1$ las restricciones.

Al escribir explícitamente el sistema de ecuaciones con los multiplicadores de Lagrange, solo en una (de las cinco ecuaciones) aparece el término n_y . Además dicha ecuación es la de forma

$$(\text{Componentes de } \mathbf{X} - \text{Multiplicador})n_y = 0,$$

por lo que para simplificar el cálculo, se escoge $n_y = 0$ como una restricción. De esta forma, (5.4.19) se reduce a

$$n_x^2 + n_z^2 = 1,$$

y al aplicar esta restricción simplificada y $n_y = 0$ a (5.4.23), se tiene

$$\mathbf{M}_{\pm} = \begin{pmatrix} 1 & \pm n_x & \pm n_z \\ \pm n_x & 1 - n_z^2 & n_x n_z \\ \pm n_z & n_x n_z & 1 - n_x^2 \end{pmatrix},$$

de esta manera se facilita el cálculo explícito de las probabilidades y concurrencias en las expresiones $G_{\mathbf{n}}$ y $R_{\mathbf{n}}$ y el sistema (5.4.28) se reduce a

$$\begin{aligned}\nabla_{\mathbf{n}}[G_{\mathbf{n}} + \mu R_{\mathbf{n}}] &= 0, \\ R_{\mathbf{n}} &= 0,\end{aligned}\tag{5.4.29}$$

con

$$\begin{aligned}G_{\mathbf{n}} &= p_{\mathbf{n}}^2 - p_{\mathbf{n}}^2 C_{\mathbf{n}}^2 \\ &= \frac{1}{4}(1 + Y_x n_x + Y_z n_z)^2 - \frac{1}{4}[X_x^2 + X_y^2 + X_z^2 + 2X_x(X_y n_x + X_z n_z) \\ &\quad - (X_y n_z - X_z n_x)^2]\end{aligned}\tag{5.4.30}$$

³Ver apéndice C

y

$$\begin{aligned}
R_{\mathbf{n}} &= p_{-\mathbf{n}}^2 C_{-\mathbf{n}}^2 - p_{-\mathbf{n}}^2 \\
&= \frac{1}{4} \left\{ (-X_z^2 - Y_x^2) n_x^2 + (-X_y^2 - Y_z^2) n_z^2 + 2(X_y X_z - Y_x Y_z) n_x n_z + 2(Y_x - X_x X_y) n_x \right. \\
&\quad \left. + 2(Y_z - X_x X_z) n_z + X_x^2 + X_y^2 + X_z^2 - 1 \right\}. \tag{5.4.31}
\end{aligned}$$

Además, de la restricción $R_{\mathbf{n}} = 0$ se obtiene

$$(X_y n_z - X_z n_x)^2 = X_x^2 + X_y^2 + X_z^2 - 2X_x(X_y n_x + X_z n_z) - (1 - Y_x n_x - Y_z n_z)^2$$

que al reemplazarlo en (5.4) se tiene que

$$G_{\mathbf{n}} = (Y_x - X_x X_y) n_x + (Y_z - X_x X_z) n_z. \tag{5.4.32}$$

De esta manera, el sistema de ecuaciones (5.4.29) se escribe explícitamente como

$$(Y_x - X_x X_y) + \mu \frac{1}{2} \{ (-X_z^2 - Y_x^2) n_x + (X_y X_z - Y_x Y_z) n_z + (Y_x - X_x X_y) \} = 0, \tag{5.4.33}$$

$$(Y_z - X_x X_z) + \mu \frac{1}{2} \{ (-X_y^2 - Y_z^2) n_z + (X_y X_z - Y_x Y_z) n_x + (Y_z - X_x X_z) \} = 0, \tag{5.4.34}$$

$$\begin{aligned}
\frac{1}{4} \left\{ (-X_z^2 - Y_x^2) n_x^2 + (-X_y^2 - Y_z^2) n_z^2 + 2(X_y X_z - Y_x Y_z) n_x n_z \right. \\
\left. + 2(Y_x - X_x X_y) n_x + 2(Y_z - X_x X_z) n_z + X_x^2 + X_y^2 + X_z^2 - 1 \right\} = 0. \tag{5.4.35}
\end{aligned}$$

Se sigue que, al despejar μ de (5.4.33) y (5.4.34) e igualar⁴, se obtiene

$$\Omega_1 n_x = \Omega_2 n_z$$

donde

$$\Omega_1 = \{ (X_z^2 + Y_x^2)(Y_z - X_x X_z) + (Y_x - X_x X_y)(X_y X_z - Y_x Y_z) \}, \tag{5.4.36}$$

$$\Omega_2 = \{ (X_y^2 + Y_z^2)(Y_x - X_x X_y) + (Y_z - X_x X_z)(X_y X_z - Y_x Y_z) \}. \tag{5.4.37}$$

A partir de aquí se tienen cuatro posibles casos:

⁴Los términos que acompañan a μ en (5.4.33) y (5.4.34), deben ser necesariamente distintos de cero, porque sino se estaría quitando la restricción $R_{\mathbf{n}} = 0$, esto es, que el estado ortogonal sea un estado de Bell.

1. $\Omega_1 = 0$ y $\Omega_2 = 0$,
2. $\Omega_1 = 0$ y $\Omega_2 \neq 0$,
3. $\Omega_1 \neq 0$ y $\Omega_2 = 0$,
4. $\Omega_1 \neq 0$ y $\Omega_2 \neq 0$.

5.4.0.1. Caso 1.

El caso 1. no aporta ninguna información.

5.4.0.2. Caso 2.

En este caso se tiene

$$0 = \Omega_2 n_z$$

cuya solución es $n_z = 0$, y dado que $n_x^2 + n_z^1 = 1$ se tiene $n_x^\pm = \pm 1$.

Al reemplazar $n_x^\pm = \pm 1$ y $n_z = 0$ en la función objetivo (5.4.32) se tiene

$$G_{\mathbf{n}}^{(2)\pm} = \pm(Y_x - X_x X_y), \quad (5.4.38)$$

y al reemplazar en la restricción (5.4.35) se tiene

$$(X_x \mp X_y)^2 - (Y_x \mp 1)^2 = 0. \quad (5.4.39)$$

5.4.0.3. Caso 3.

En este caso se tiene

$$\Omega_1 n_x = 0$$

cuya solución es $n_x = 0$, y dado que $n_x^2 + n_z^1 = 1$ se tiene $n_z^\pm = \pm 1$.

Al reemplazar $n_x = 0$ y $n_z^\pm = \pm 1$ en la función objetivo (5.4.32) se tiene

$$G_{\mathbf{n}}^{(3)\pm} = \pm(Y_z - X_x X_z), \quad (5.4.40)$$

y al reemplazar en la restricción (5.4.35) se tiene

$$(X_x \mp X_z)^2 - (Y_z \mp 1)^2 = 0. \quad (5.4.41)$$

5.4.0.4. Caso 4.

En este caso se tiene

$$n_x = \frac{\Omega_2}{\Omega_1} n_z = K n_z, \quad (5.4.42)$$

donde se ha definido

$$K = \frac{\Omega_2}{\Omega_1} = \frac{(X_y^2 + Y_z^2)(Y_x - X_x X_y) + (Y_z - X_x X_z)(X_y X_z - Y_x Y_z)}{(X_z^2 + Y_x^2)(Y_z - X_x X_z) + (Y_x - X_x X_y)(X_y X_z - Y_x Y_z)}.$$

Al reemplazar $n_x = K n_z$ en la función objetivo (5.4.32) se tiene

$$G_n^{(4)} = \{K(Y_x - X_x X_y) + (Y_z - X_x X_z)\} n_z, \quad (5.4.43)$$

y al reemplazar en la restricción (5.4.35) se obtiene

$$\begin{aligned} & -\{K^2(X_z^2 + Y_x^2) - 2K(X_y X_z - Y_x Y_z) + (X_y^2 + Y_z^2)\} n_z^2 \\ & + 2\{K(Y_x - X_x X_y) + (Y_z - X_x X_z)\} n_z + X_x^2 + X_y^2 + X_z^2 - 1 = 0. \end{aligned} \quad (5.4.44)$$

Definiendo

$$a = K^2(X_z^2 + Y_x^2) - 2K(X_y X_z - Y_x Y_z) + (X_y^2 + Y_z^2), \quad (5.4.45)$$

$$b = K(Y_x - X_x X_y) + (Y_z - X_x X_z), \quad (5.4.46)$$

$$c = X_x^2 + X_y^2 + X_z^2 - 1, \quad (5.4.47)$$

se reescribe (5.4.44) como

$$-a n_z^2 + 2b n_z + c = 0,$$

que tiene dos posibles soluciones:

- Si $a \neq 0$ y $b^2 + ac \geq 0$, entonces

$$n_z^\pm = \frac{b \mp \sqrt{b^2 + ac}}{a}.$$

- Si $a = 0$, entonces


$$n_z = -\frac{c}{2b}.$$

Al reemplazar estas soluciones de n_z en la función objetivo⁵ (5.4.43) se obtiene:

- Si $a \neq 0$ y $b^2 + ac \geq 0$, entonces

$$G_{\mathbf{n}}^{(4,1)\pm} = \frac{b^2 \mp b\sqrt{b^2 + ac}}{a}. \quad (5.4.48)$$

- Si $a = 0$, entonces



$$G_{\mathbf{n}}^{(4,2)} = -\frac{c}{2}. \quad (5.4.49)$$

5.4.1. Máxima probabilidad de éxito Estrategia 2

Finalmente, la solución al problema de minimización es

$$G_{\mathbf{n}}^{\min} = \begin{cases} G_{\mathbf{n}}^{(2)\pm}, & \text{si } \Omega_1 = 0, H^{(2)} = 0. \\ G_{\mathbf{n}}^{(3)\pm}, & \text{si } \Omega_2 = 0, H^{(3)} = 0. \\ G_{\mathbf{n}}^{(4,1)\pm}, & \text{si } \Omega_{1,2} \neq 0, a \neq 0, b^2 + ac \geq 0. \\ G_{\mathbf{n}}^{(4,2)}, & \text{si } \Omega_{1,2} \neq 0, a \neq 0. \end{cases} \quad (5.4.50)$$

Con

$$\begin{aligned} G_{\mathbf{n}}^{(2)\pm} &= \pm(Y_x - X_x X_y), \\ G_{\mathbf{n}}^{(3)\pm} &= \pm(Y_z - X_x X_z), \\ G_{\mathbf{n}}^{(4,1)\pm} &= \frac{b^2 \mp b\sqrt{b^2 + ac}}{a}, \\ G_{\mathbf{n}}^{(4,2)} &= -\frac{c}{2}, \end{aligned}$$

⁵Se debe notar que (5.4.43) se puede reescribir usando la definición de b en (5.4.46), es decir $G_{\mathbf{n}}^{(4)} = bn_z$.

$$\Omega_1 = (X_z^2 + Y_x^2)(Y_z - X_x X_z) + (Y_x - X_x X_y)(X_y X_z - Y_x Y_z),$$

$$\Omega_2 = (X_y^2 + Y_z^2)(Y_x - X_x X_y) + (Y_z - X_x X_z)(X_y X_z - Y_x Y_z),$$

$$H^{(2)} = (X_x \mp X_y)^2 - (Y_x \mp 1)^2,$$

$$H^{(3)} = (X_x \mp X_z)^2 - (Y_z \mp 1)^2,$$

$$a = K^2(X_z^2 + Y_x^2) - 2K(X_y X_z - Y_x Y_z) + (X_y^2 + Y_z^2),$$

$$b = K(Y_x - X_x X_y) + (Y_z - X_x X_z),$$

$$c = X_x^2 + X_y^2 + X_z^2 - 1,$$

$$K = \frac{(X_y^2 + Y_z^2)(Y_x - X_x X_y) + (Y_z - X_x X_z)(X_y X_z - Y_x Y_z)}{(X_z^2 + Y_x^2)(Y_z - X_x X_z) + (Y_x - X_x X_y)(X_y X_z - Y_x Y_z)},$$

y X_i e Y_j con $i, j = x, y, z$ son las componentes de \mathbf{X} y \mathbf{Y} definidos en (5.4.21) y (5.4.22).

De esta forma, la máxima probabilidad de éxito de la Estrategia 2 (5.4.11) viene dada por

$$p_{\text{éxito}}^{(2)} = 1 - \sqrt{G_{\mathbf{n}}^{\text{mín}}}. \quad (5.4.51)$$

5.5. Comparación

Para generar un estado de Bell (es decir, un estado maximalmente entrelazado) a partir de un estado puro tripartito de parámetros reales, es posible emplear dos estrategias, las que se desarrollaron en las secciones precedentes y se resumen a continuación.

5.5.1. Estrategia 1

1. Se aplica el esquema de Extracción Determinista de Entrelazamiento sobre el estado tripartito inicial, lo que resulta en dos posibles estados bipartitos puros de salida, ambos con la misma concurrencia C_d .

2. Sobre estos estados se aplica el método Procusteano.
3. La máxima probabilidad de éxito $p_{\text{éxito}}^{(1)}$ de esta estrategia es dada por (5.3.1).

5.5.2. Estrategia 2

1. Se realiza una medición local sobre un qubit del estado tripartito inicial utilizando la base $\{|\theta, \phi\rangle, |\theta + \pi, \phi\rangle\}$.
2. Se busca el conjunto de ángulos $\{\theta_s, \phi_s\}$ tal que uno de los estados resultantes de la medición sea maximalmente entrelazado ($C_{\theta_s+\pi, \phi_s} = 1$).
3. Para el mismo conjunto de ángulos, el otro estado resultante de la medición no será maximalmente entrelazado ($C_{\theta_s, \phi_s} \neq 1$).
4. Sobre el estado no maximalmente entrelazado se aplica el Método Procusteano.
5. La máxima probabilidad de éxito $p_{\text{éxito}}^{(2)}$ de esta estrategia es dada por (5.4.51).

5.5.2.1. Comparación numérica y comparación entre estrategias

Se han descrito los pasos necesarios para realizar cada estrategia. Siguiendo la secuencia de la Estrategia 2, se calculará de forma numérica la probabilidad de éxito, además se resolverá de forma numérica el sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35) que lleva a la máxima probabilidad de éxito, y se compararán los resultados con el resultado analítico (5.4.51).

Por otra parte, se compararán las máximas probabilidades de éxito de la Estrategia 1 y Estrategia 2 para generar estados de Bell a partir de un estado tripartito.

5.5.3. Estado Tripartito Inicial

Para llevar a cabo las comparaciones se utilizará el estado tripartito inicial

$$|\psi\rangle = z \left(\alpha |\text{GHZ}_+\rangle + \sqrt{1 - \alpha^2} |\text{GHZ}_-\rangle \right) + \sqrt{1 - z^2} \left(\beta |\text{W}_2\rangle + \sqrt{1 - \beta^2} |\text{W}_1\rangle \right),$$

con $z \in [-1, 1]$, $\alpha \in [-1, 1]$ y $\beta \in [-1, 1]$, y

$$\begin{aligned} |W_1\rangle &= \frac{|001\rangle + |010\rangle + |100\rangle}{\sqrt{3}}, \\ |W_2\rangle &= \frac{|101\rangle + |011\rangle + |011\rangle}{\sqrt{3}}, \\ |\text{GHZ}_{\pm}\rangle &= \frac{|000\rangle + |111\rangle}{\sqrt{2}}. \end{aligned}$$

Al calcular las componentes de \mathbf{X} y \mathbf{Y} utilizando (5.4.21) y (5.4.22) se obtiene

$$X_x = \frac{2}{3}(1-z^2) - \sqrt{\frac{2}{3}}z\sqrt{1-z^2}\left[(\alpha + \sqrt{1-\alpha^2})\beta + (\alpha - \sqrt{1-\alpha^2})\sqrt{1-\beta^2}\right] \quad (5.5.1)$$

$$X_y = \frac{2}{3}(1-z^2)\beta\sqrt{1-\beta^2} + z^2(1-2\alpha^2) \quad (5.5.2)$$

$$X_z = \frac{2}{3}(1-z^2)(1-2\beta^2) - \sqrt{\frac{2}{3}}z\sqrt{1-z^2}\left[(\alpha + \sqrt{1-\alpha^2})\beta - (\alpha - \sqrt{1-\alpha^2})\sqrt{1-\beta^2}\right] \quad (5.5.3)$$

$$Y_x = \frac{4}{3}(1-z^2)\beta\sqrt{1-\beta^2} + \sqrt{\frac{2}{3}}z\sqrt{1-z^2}\left[(\alpha - \sqrt{1-\alpha^2})\beta + (\alpha + \sqrt{1-\alpha^2})\sqrt{1-\beta^2}\right] \quad (5.5.4)$$

$$Y_y = 0, \quad (5.5.5)$$

$$Y_z = 2z^2\alpha\sqrt{1-\alpha^2} + \frac{1}{3}(1-z^2)(1-2\beta^2). \quad (5.5.6)$$

5.5.4. Caso $\alpha = 1$ y $\beta = 0$

En este caso el estado inicial queda de la forma

$$|\psi\rangle = z\left(\alpha|\text{GHZ}_+\rangle + \sqrt{1-\alpha^2}|\text{GHZ}_-\rangle\right) + \sqrt{1-z^2}\left(\beta|W_2\rangle + \sqrt{1-\beta^2}|W_1\rangle\right),$$

y las componentes de \mathbf{X} e \mathbf{Y} son

$$\begin{aligned}
 X_x &= \frac{2}{3}(1 - z^2) - \sqrt{\frac{2}{3}}z\sqrt{1 - z^2}, \\
 X_y &= -z^2, \\
 X_z &= \frac{2}{3}(1 - z^2) + \sqrt{\frac{2}{3}}z\sqrt{1 - z^2}, \\
 Y_x &= \frac{2}{3}z\sqrt{1 - z^2}, \\
 Y_z &= \frac{1}{3}(1 - z^2).
 \end{aligned} \tag{5.5.7}$$

Se utiliza (5.5.7) para calcular la probabilidad de éxito de la Estrategia 2 siguiendo la secuencia de pasos descritos en 5.5.2, también se utiliza para resolver numéricamente el sistema de ecuaciones (5.4.33)-(5.4.35) y para calcular la máxima probabilidad de éxito $p_{\text{éxito}}^2$ dada por (5.4.51). La implementación de estas formas de calcular la probabilidad se realiza por medio del computador. En la figura 5.5.1 se pueden ver los resultados obtenidos.

El gráfico gris en la figura 5.5.1 es la probabilidad que se obtiene realizando la estrategia de forma secuencial. Se puede apreciar que esta gráfica tiene ancho, esto es debido al error numérico al buscar el conjunto de ángulos que haga $C_{\theta+\pi,\phi} = 1$.

El gráfico azul en la figura 5.5.1 es la probabilidad que se obtiene a partir de solucionar numéricamente el sistema de ecuaciones antes mencionado. Se puede apreciar una pequeña discontinuidad en $z \approx 0,50$, esto es debido a error numérico y probablemente a divisiones por términos cercanos a cero.

El gráfico verde en la figura 5.5.1 es la probabilidad que se obtiene al utilizar la expresión (5.4.51) para calcular $p_{\text{éxito}}^2$ de la Estrategia 2.

En la figura 5.5.1 se ve en el gráfico comparativo, que en todas las formas de llegar a la probabilidad de éxito de la Estrategia 2 se obtiene el mismo resultado, salvo diferencias debido a error numérico.

Por otro lado, en la figura 5.5.2 se tiene una gráfica comparativa de las probabilidades de éxito de cada estrategia, estas se obtuvieron haciendo uso de (5.5.7) en el cálculo de $p_{\text{éxito}}^{(1)}$ dada en (5.3.1) y $p_{\text{éxito}}^{(2)}$ dada en (5.4.51). De esta

figura se ve claramente que la Estrategia 2 es la que tiene mayor probabilidad de éxito en generar un estado de Bell, siendo esta probabilidad mayor al 50 %, y que ambas probabilidades se solapan entre $z \approx 0,50$ y $z \approx 0,75$.



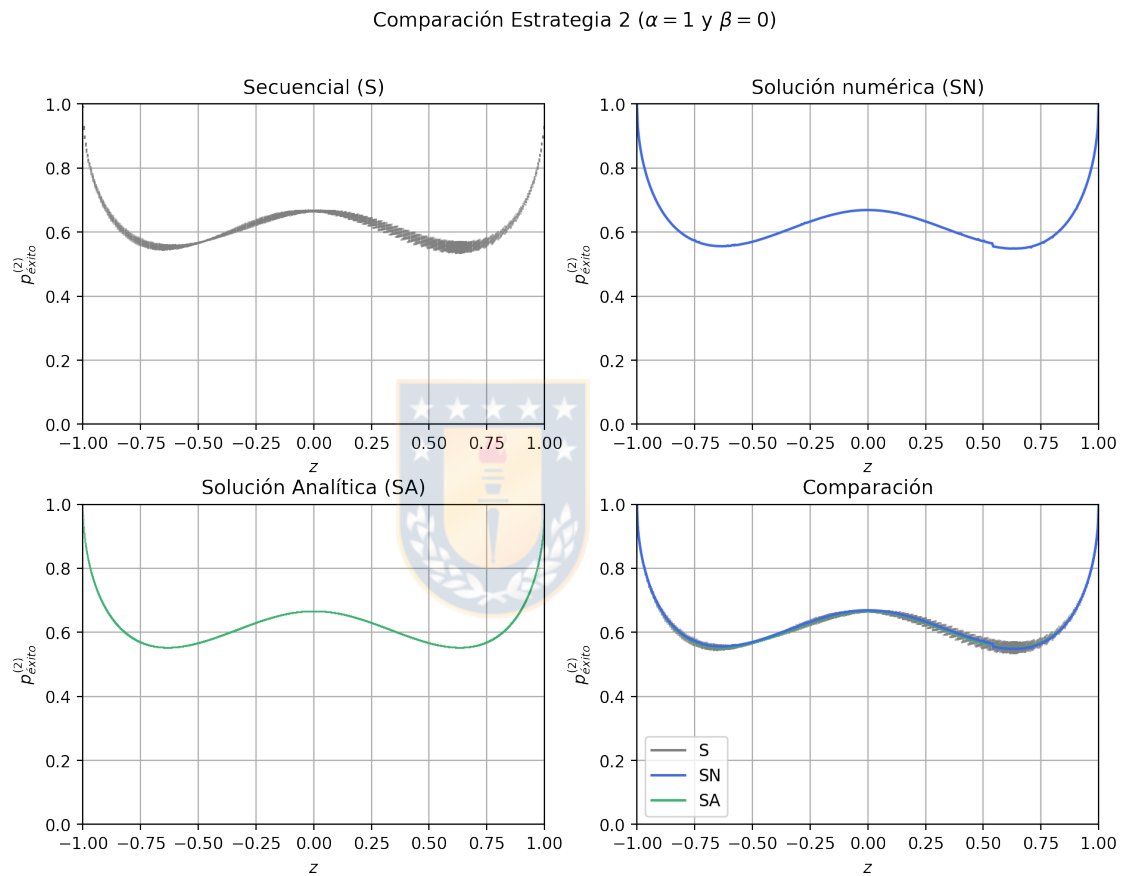


Figura 5.5.1: [$\alpha = 1$, $\beta = 0$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. **Secuencial (S):** Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. **Solución numérica (SN):** Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Solución Analítica (SA):** Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Comparación:** Probabilidad de éxito estrategia 2 obtenida de distintos modos. *Fuente: Elaborado por el autor.*

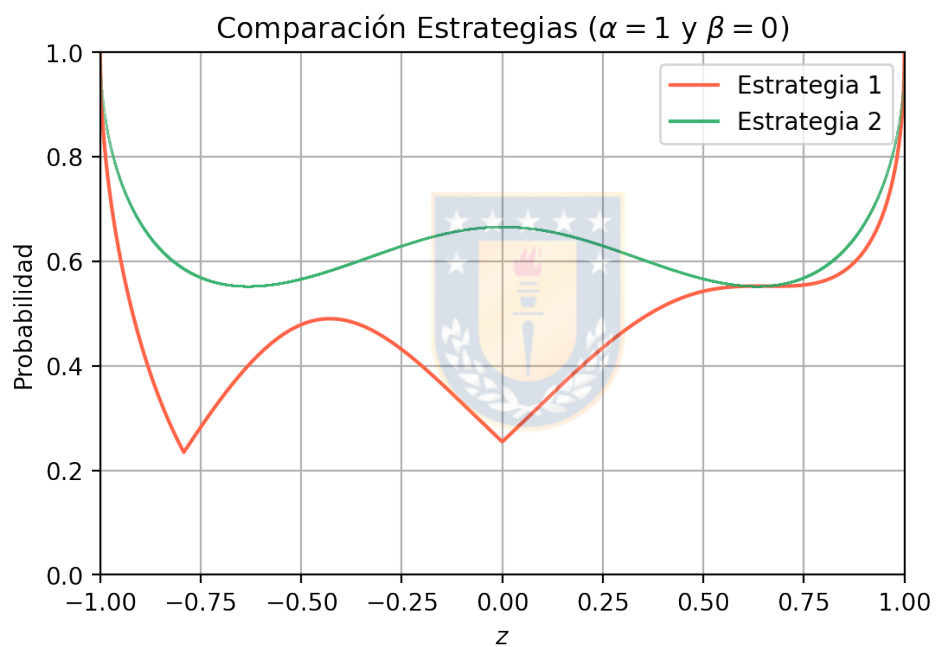


Figura 5.5.2: [$\alpha = 1$, $\beta = 0$] Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde). *Fuente: Elaborado por el autor.*

5.5.5. Caso $\alpha = 1/2$ y $\beta = 1/2$

En este caso el estado inicial queda de la forma

$$|\psi\rangle = \frac{z}{2} \left(|\text{GHZ}_+\rangle + \sqrt{3} |\text{GHZ}_-\rangle \right) + \frac{\sqrt{1-z^2}}{2} \left(|W_2\rangle + \sqrt{3} |W_1\rangle \right),$$

y las componentes de \mathbf{X} e \mathbf{Y} son

$$\begin{aligned} X_x &= \frac{2}{3}(1-z^2) + \sqrt{\frac{2}{3}}z\sqrt{1-z^2} \left(\frac{1-\sqrt{3}}{2} \right), \\ X_y &= \frac{\sqrt{3}}{6}(1-z^2) + \frac{z^2}{2}, \\ X_z &= \frac{1}{3}(1-z^2) - \sqrt{\frac{2}{3}}z\sqrt{1-z^2}, \\ Y_x &= \frac{\sqrt{3}}{3}(1-z^2) + \frac{2}{3}z\sqrt{1-z^2}, \\ Y_z &= z^2 \frac{\sqrt{3}}{2} + \frac{1}{6}(1-z^2). \end{aligned} \tag{5.5.8}$$

Se utiliza (5.5.8) para calcular la probabilidad de éxito de la Estrategia 2 siguiendo la secuencia de pasos descritos en 5.5.2, también se utiliza para resolver numéricamente el sistema de ecuaciones (5.4.33)-(5.4.35) y para calcular la máxima probabilidad de éxito $p_{\text{éxito}}^2$ dada por (5.4.51). La implementación de estas formas de calcular la probabilidad se realiza por medio del computador. En la figura 5.5.3 se pueden ver los resultados obtenidos.

El gráfico gris en la figura 5.5.3 es la probabilidad que se obtiene realizando la estrategia de forma secuencial. Se puede apreciar que esta gráfica tiene ancho, esto es debido al error numérico al buscar el conjunto de ángulos que haga $C_{\theta+\pi,\phi} = 1$.

El gráfico azul en la figura 5.5.3 es la probabilidad que se obtiene a partir de solucionar numéricamente el sistema de ecuaciones antes mencionado. Se puede apreciar una pequeña discontinuidad en $z \approx 0,75$, esto es debido a error numérico y probablemente a divisiones por términos cercanos a cero.

El gráfico verde en la figura 5.5.3 es la probabilidad que se obtiene al utilizar la expresión (5.4.51) para calcular $p_{\text{éxito}}^2$ de la Estrategia 2.

En la figura 5.5.3 se ve en el gráfico comparativo, que en todas las formas de llegar

a la probabilidad de éxito de la Estrategia 2 se obtiene el mismo resultado, salvo diferencias debido a error numérico.

Por otro lado, en la figura 5.5.4 se tiene una gráfica comparativa de las probabilidades de éxito de cada estrategia, estas se obtuvieron haciendo uso de (5.5.7) en el cálculo de $p_{\text{éxito}}^{(1)}$ dada en (5.3.1) y $p_{\text{éxito}}^{(2)}$ dada en (5.4.51). De esta figura se ve que la Estrategia 2 es la que tiene mayor probabilidad de éxito en generar un estado de Bell, siendo esta probabilidad mayor al 10% para todo valor de z , en particular siendo mayor al 30% en el intervalo entre $z \approx -0,75$ y $z \approx 0,00$. El mayor valor que alcanza la probabilidad de la Estrategia 1 es de 30% en $z \approx 0,60$ y en $z \approx -0,25$. Ambas probabilidades se solapan para los valores extremos de z .



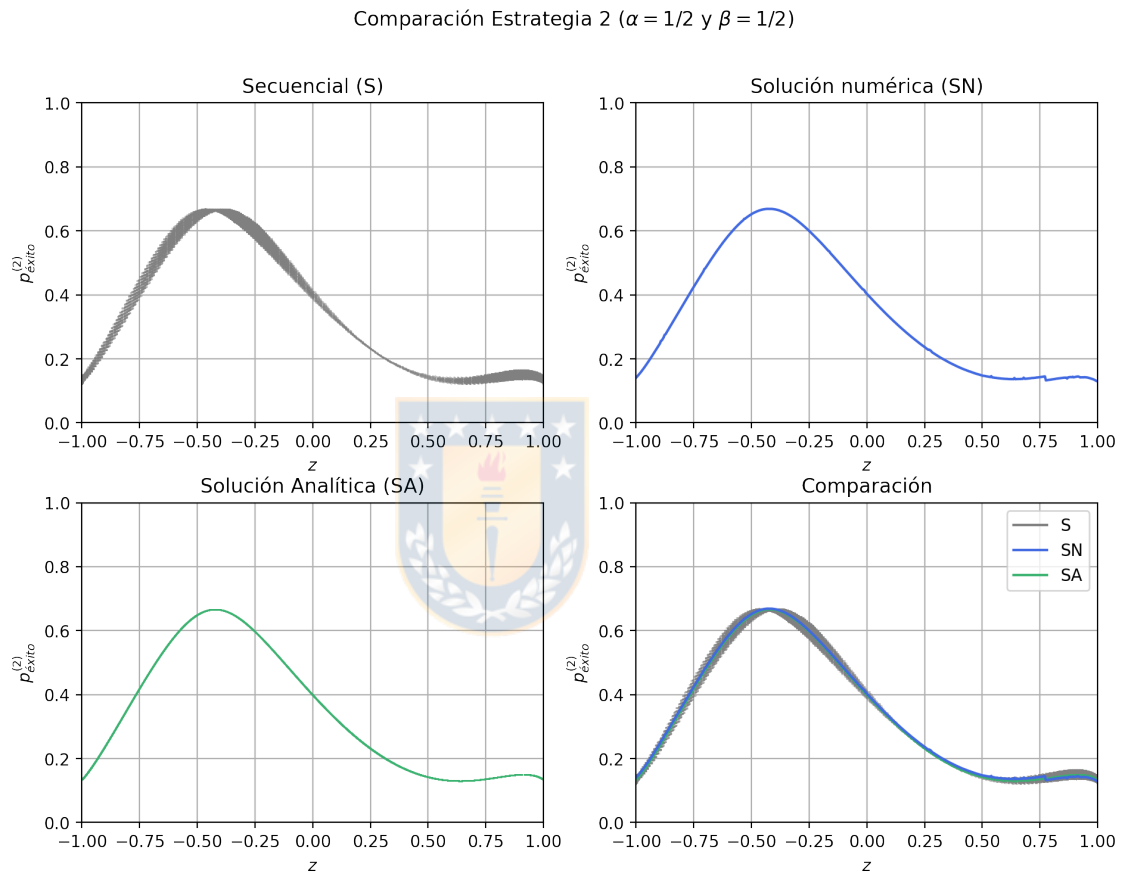


Figura 5.5.3: [$\alpha = 1/2$, $\beta = 1/2$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. **Secuencial (S):** Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. **Solución numérica (SN):** Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Solución Analítica (SA):** Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Comparación:** Probabilidad de éxito estrategia 2 obtenida de distintos modos. *Fuente: Elaborado por el autor.*

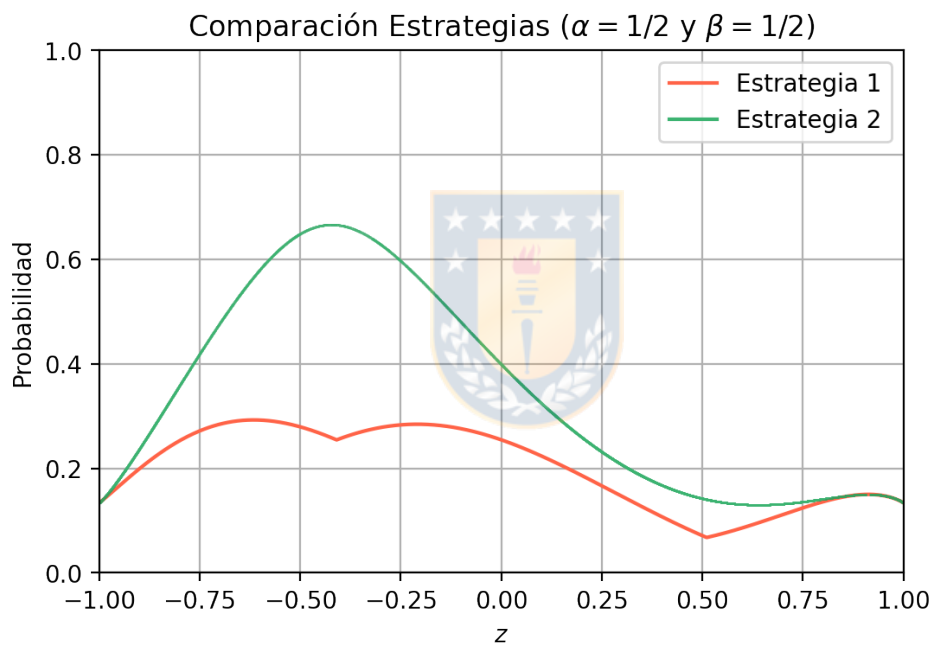


Figura 5.5.4: [$\alpha = 1/2$, $\beta = 1/2$] Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde).
Fuente: Elaborado por el autor.

5.5.6. Caso $\alpha = -1/\sqrt{6}$ y $\beta = -1/\sqrt{2}$

En este caso el estado inicial queda como

$$|\psi\rangle = -\frac{z}{\sqrt{6}} \left(|\text{GHZ}_+\rangle - \sqrt{5} |\text{GHZ}_-\rangle \right) - \frac{\sqrt{1-z^2}}{\sqrt{2}} (|W_2\rangle - |W_1\rangle),$$

y las componentes de \mathbf{X} e \mathbf{Y} son

$$\begin{aligned} X_x &= \frac{2}{3}(1-z^2) + \sqrt{10}z\sqrt{1-z^2}, \\ X_y &= -\frac{1}{3}(1-z^2) + \frac{2}{3}z^2, \\ X_z &= -\sqrt{\frac{2}{3}}z\sqrt{1-z^2}, \\ Y_x &= -\frac{2}{3}(1-z^2) + \frac{\sqrt{10}}{3}z\sqrt{1-z^2}, \\ Y_z &= -\frac{\sqrt{5}}{2}z^2. \end{aligned}$$

Se utiliza (5.5.8) para calcular la probabilidad de éxito de la Estrategia 2 siguiendo la secuencia de pasos descritos en 5.5.2, también se utiliza para resolver numéricamente el sistema de ecuaciones (5.4.33)-(5.4.35) y para calcular la máxima probabilidad de éxito $p_{\text{éxito}}^2$ dada por (5.4.51). La implementación de estas formas de calcular la probabilidad se realiza por medio del computador. En la figura 5.5.5 se pueden ver los resultados obtenidos.

El gráfico gris en la figura 5.5.5 es la probabilidad que se obtiene realizando la estrategia de forma secuencial. Se puede apreciar que esta gráfica tiene ancho, esto es debido al error numérico al buscar el conjunto de ángulos que haga $C_{\theta+\pi,\phi} = 1$.

El gráfico azul en la figura 5.5.5 es la probabilidad que se obtiene a partir de solucionar numéricamente el sistema de ecuaciones antes mencionado. Se puede apreciar una pequeña discontinuidad en $z \approx -0,80$, esto es debido a error numérico y probablemente a divisiones por términos cercanos a cero.

El gráfico verde en la figura 5.5.5 es la probabilidad que se obtiene al utilizar la expresión (5.4.51) para calcular $p_{\text{éxito}}^2$ de la Estrategia 2.

En la figura 5.5.5 se ve en el gráfico comparativo, que en todas las formas de llegar

a la probabilidad de éxito de la Estrategia 2 se obtiene el mismo resultado, salvo diferencias debido a error numérico.

Por otro lado, en la figura 5.5.6 se tiene una gráfica comparativa de las probabilidades de éxito de cada estrategia, estas se obtuvieron haciendo uso de (5.5.7) en el cálculo de $p_{\text{éxito}}^{(1)}$ dada en (5.3.1) y $p_{\text{éxito}}^{(2)}$ dada en (5.4.51). De esta figura se ve que la Estrategia 2 es la que tiene mayor probabilidad de éxito en generar un estado de Bell, siendo esta probabilidad mayor al 20 % en más de la mitad de los valores de z , específicamente entre $z \approx -0,10$ y $z \approx 1,00$. Además, se puede apreciar que ambas estrategias alcanzan su mínimo y máximo valor de probabilidad aproximadamente para los mismos valores de z , a saber, $z \approx -0,50$ para el mínimo y $z \approx 0,50$ para el máximo. Siendo el valor mínimo de probabilidad cercano a 0 % para ambas estrategias, y el valor máximo de probabilidad cercano al 70 % para la Estrategia 1 y cercano al 80 % para la Estrategia 2.



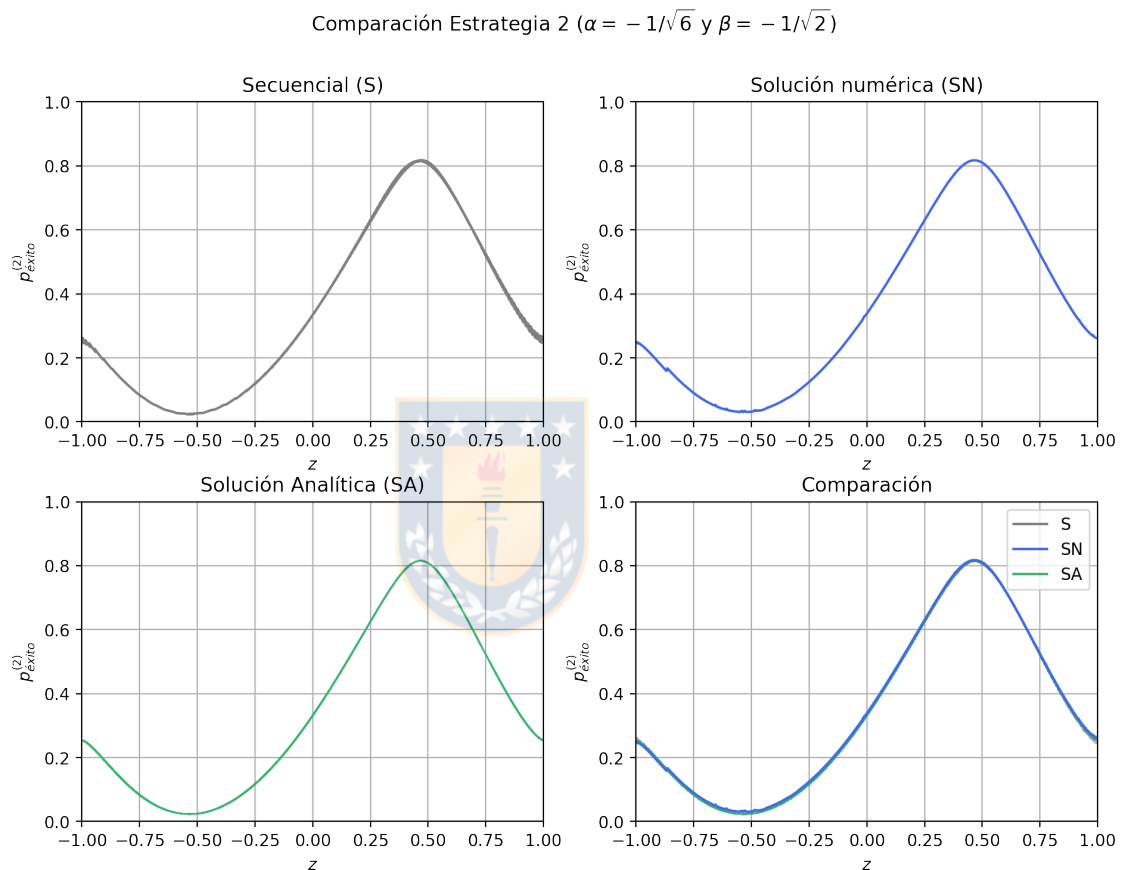


Figura 5.5.5: [$\alpha = -1/\sqrt{6}$, $\beta = -1/\sqrt{2}$] Gráficos de la probabilidad de éxito de la Estrategia 2 obtenidos de distintas formas. **Secuencial (S):** Gráfico obtenido realizando numéricamente la secuencia descrita en 5.5.2. **Solución numérica (SN):** Gráfico obtenido de la solución numérica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Solución Analítica (SA):** Gráfico obtenido de la solución analítica del sistema de ecuaciones (5.4.33), (5.4.34) y (5.4.35). **Comparación:** Probabilidad de éxito estrategia 2 obtenida de distintos modos. Fuente: Elaborado por el autor.

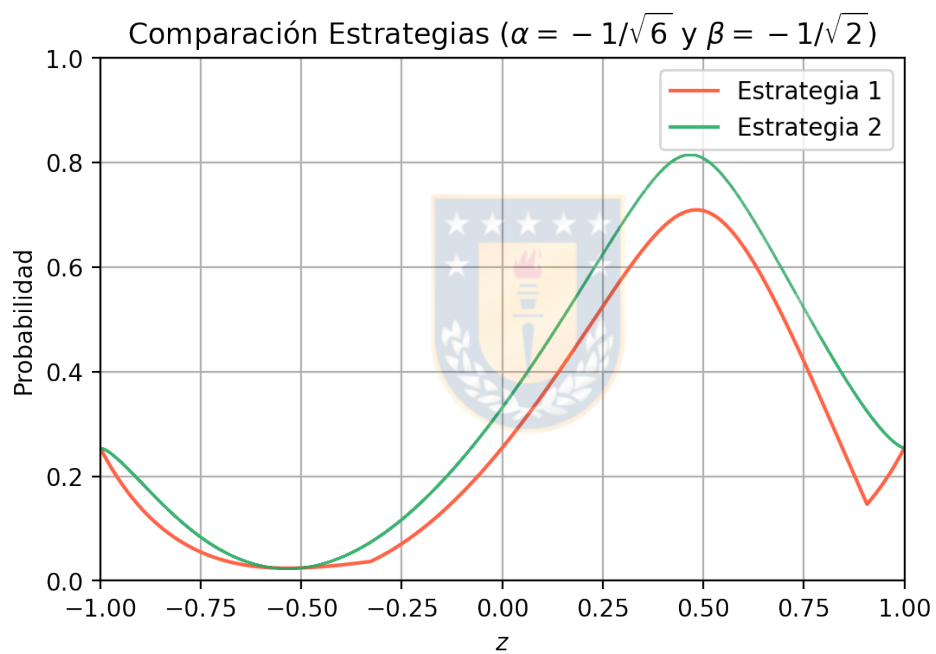


Figura 5.5.6: $[\alpha = -1/\sqrt{6}, \beta = -1/\sqrt{2}]$ Comparación entre máxima probabilidad de éxito Estrategia 1 (rojo) y máxima probabilidad de éxito Estrategia 2 (verde). Fuente: Elaborado por el autor.

Capítulo 6

Conclusión

En el presente trabajo se desarrollaron y compararon dos estrategias para generar probabilísticamente estados de Bell a partir de un estado tripartito puro.

La primera estrategia que se elaboró, consistía en utilizar un proceso de Extracción de Entrelazamiento Determinista a un estado tripartito, y sobre los estados resultantes aplicar un óptimo método Procusteano. Se encontró una expresión analítica para determinar la máxima probabilidad de éxito de esta estrategia.

La segunda estrategia que se desarrolló, consistía en realizar una medición local sobre un qubit del estado tripartito puro, la medición se lleva a cabo utilizando una base ortonormal parametrizada por ángulos. Para los posibles estados bipartitos resultantes de esta medición local, se busca el conjunto de ángulos que hace uno de los estados de salida maximalmente entrelazado. Para el mismo conjunto de ángulos, el estado bipartito ortogonal estará parcialmente entrelazado, por lo que sobre él se aplica el método Procusteano. Se encontró una expresión analítica para calcular la máxima probabilidad de éxito de esta estrategia.

Para poder hallar la expresión analítica de la máxima probabilidad de éxito de la segunda estrategia, fue necesario realizar un proceso de minimización sobre una función que dependía de los ángulos de la base de medición.

Finalmente, se utilizó un estado tripartito particular para comparar ambas estrategias desarrolladas. Además, haciendo uso del mismo estado, se compararon los resultados analíticos y numéricos de la segunda estrategia.

Al comparar las dos estrategias para distintos casos, se encontró que la segunda estrategia es la que tiene mayor o igual probabilidad de éxito que la primera estrategia para generar estado de Bell.

Si bien en los casos probados, la segunda estrategia es la que tiene mayor o igual probabilidad de éxito de generar un estado Bell, es necesario obtener una desigualdad general para asegurar que siempre esta estrategia es la óptima.

Futuros trabajos a partir de este son diseñar experimentos para implementar estas estrategias, extender las estrategias a estados tripartitos mixtos y relacionar la máxima probabilidad de éxito de la segunda estrategia con las correlaciones cuánticas presentes en el estado tripartito inicial.



Bibliografía

- [1] Hassani, S. (2009). *Mathematical Methods for Students of Physics and Related Fields* (2a. ed.). Normal, Illinois: Springer.
- [2] Bertsekas, D. P. y Tsitsiklis J. N. (2008). *Introduction to Probability* (2a. ed.). Belmont, Massachusetts: Athena Scientific.
- [3] Ross, S. (2009). *A First Course in Probability* (8a. ed.). Upper Saddle River, New Jersey: Prentice Hall.
- [4] de la Peña, L. (2014). *Introducción a la Mecánica Cuántica* (1a. ed.). Edición Electrónica, Ediciones Científicas Universitarias, Fondo de Cultura Económica, Mexico.
- [5] Nielsen, M. A. y Chuang, I.L. (2010). *Quantum Computation and Quantum Information* (10a. ed.). United Kingdom: Cambridge University Press.
- [6] Renes, J. M. (2014). *Quantum Information Theory*. Recuperado el 02 de marzo de 2020, del sitio Web de la Universidad Escuela Politécnica Federal de Zúrich: http://edu.itp.phys.ethz.ch/hs15/QIT/renes_lecture_notes14.pdf
- [7] Barnett, S. M. (2009). *Quantum Information* (1a. ed.). Gran Bretaña: Oxford U. Press.
- [8] Bennet, C. H. y DiVicenzo, D. P. (2000). Quantum information and computation. *Nature*, 404, 247-256.
- [9] Alber, G., Beth. T, Horodecki, M., Horodecki, P., Horodecki, R., Röttler, M., Weinfurter, H., Werner, R. y Zeilinger, A. (2001). *Quantum Information: An Introduction to Basic Theoretical Concepts and Experiments*. Alemania: Springer.
- [10] Schumacher, B. (1995). Quantum Coding. *Phys. Rev. A*, 51(4), 2738-2747.
- [11] Ariana, M. (2014). *Swapping de Correlaciones Cuánticas*. Trabajo de grado, Magíster en Ciencias mención en Física, Universidad de Concepción, Concepción.
- [12] Mermin, N.D. (2007). *Quantum Computer Science: An Introduction* (1a ed.). Cambridge: Cambridge University Press.

- [13] Streltsov, A. (2015). *Quantum Correlations Beyond Entanglement and Their Role in Quantum Information Theory (1a. ed.)*. Springer.
- [14] Shor, P. W. *Algorithms for quantum computation: discrete logarithms and factoring*, Proceedings 35th Annual Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 1994, pp. 124-134.
- [15] Grover, L. K. *A fast quantum mechanical algorithm for database search*, Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96). Association for Computing Machinery, New York, NY, USA, 1996, pp. 212–219.
- [16] Grover, L. K. (1997). Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Phys. Rev. Lett.*, *79*(2), 325-328.
- [17] Bennet, C. H., DiVincenzo, D. P., Shor, P. W., Smolin, J. A., Terhal, B. M. y Wootters, W. K. (2001). Remote state preparation. *Phys. Rev. Lett.*, *87*(7), 077902.
- [18] Lo, H. K. (2000). Classical-communication cost in distributed quantum-information processing: A generalization of quantum-communication complexity. *Phys. Rev. A*, *62*(1), 012313.
- [19] Pati, A. K. (2000). Minimum classical bit for remote preparatino and measurement of a qubit. *Phys. Rev. A*, *63*(1), 014302.
- [20] Bennet, C. H. y Wiesner, S. J. (1992). Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.*, *69*(20), 2881-2884.
- [21] Charles H. Bennet, Gilles Brassad, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, *70*:1895-1899, Mar 1993.
- [22] Zukowski, M., Zeilinger, A., Horne, M. A. y Ekert, A. K. (1993). “Event-ready-detectors” Bell experiment via entanglement swapping. *Phys. Rev. Lett.*, *71*(26), 4287-4290.
- [23] Gisin, N., Ribordy, G., Tittel, W. y Zbinden, H. (2002). Quantum cryptography. *Rev. Mod. Phys.*, *74*(1), 145-195.
- [24] Jiménez, O. (2009). *Aplicaciones de la discriminación de estados cuánticos*. Trabajo de grado, Doctor en Ciencias con Mención en Física, Universidad de Concepción, Concepción.
- [25] Schrödinger, E. (1935). Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, *31*(4), 555-563.

- [26] Einstein, A., Podolsky, B. y Rosen N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, *47*, 777-780.
- [27] Bohr, N. (1935). Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, *48*, 69-702.
- [28] Bohm, D. (1952). A suggested interpretation of the quantum theory in terms of “hidden” variables. *Phys. Rev.*, *85*(2), 166-179.
- [29] Bell, J. S. (1964). On the Einstein-Podolsky-Rosen paradox. *Physics*, *1*(3), 195-200.
- [30] Werner, R. F. (1989). Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, *40*(8), 4277-4281.
- [31] Schumacher, B. y Westmoreland, M. (2010). *Quantum Processes, Systems and Information* (1a. ed.). United Kingdom: Cambridge University Press.
- [32] Bruss, D., D’Ariano, G., Macchiavello, C. y Sacchi, M. F. (2000). Approximate quantum cloning and the impossibility of superluminal information transfer. *Phys. Rev. A*, *62*, 062302.
- [33] Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. y Wootters, W. K. (1996). Mixed-state entanglement and quantum error correction. *Phys. Rev. A*, *54*(5), 3824-3851.
- [34] Chitambar, E., Leung, D., Mančinska, L., Ozols, M. y Winter, A. (2014). Everything you always wanted to know about LOCC (but were afraid to ask). *Commun. Math. Phys.*, *328*(5), 303-326.
- [35] Horodecki, R., Horodecki, P., Horodecki, M. y Horodecki, K. (2009). Quantum entanglement. *Rev. Mod. Phys.*, *81*(2), 865-942.
- [36] Bennett, C. H., Bernstein, H. J., Popescu, S. y Schumacher, B. (1996). Concentrating partial entanglement by local operations. *Phys. Rev. A*, *53*(4), 2046-2052.
- [37] Bennett, C. H., Brassard, G., Popescu, S. y Schumacher, B. (1996). Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels. *Phys. Rev. Lett.*, *76*(5), 722-725.
- [38] M. S., David (2021). *Te saludo, persona que está revisando las referencias. Espero te sean de utilidad.* Trabajo de grado, Magíster en Ciencias con Mención en Física, Universidad de Concepción, Concepción.
- [39] Plenio, M. B. y Virmani, S. (2007). An introduction to entanglement measures. *Quantum Information & Computation*, *71*(1), 1-51.
- [40] Bruß, D. (2002). Characterizing entanglement. *Journal of Mathematical Physics*, *43*(9), 4237-4251.

- [41] Uhlmann, A. (1989). Entropy and optimal decompositions of states relative to a maximal commutative subalgebra. *Open Syst. Inf. Dyn.*, 5, 209-228.
- [42] Wootters, W. K. (1998). Entanglement of formation of an arbitrary state of two qubits. *Phys. Rev. Lett.*, 80(10), 2245-2248.
- [43] Jara, C. (2013). *Generación y Modificación de Correlaciones Cuánticas*. Trabajo de título, Físico, Universidad de Concepción, Concepción.
- [44] Modi, K., Paterek, T., Son, W., Vedral, V. y Williamson, M. (2010). Unified view of quantum and classical correlations. *Phys. Rev. Lett.*, 104, 080501.
- [45] Coffman, V., Kundu, J. y Wootters, W. K. (2000). Distributed entanglement. *Phys. Rev. A*, 61(5), 052306.
- [46] Roa, L., Muñoz, A., Muñoz, C. y Klimov, A. B. (2019). Deterministic entanglement extraction. *Phys. Rev. A*, 99(5), 052344.
- [47] Lo, H-K., Popescu, S. y Spiller, R. (2001). *Introduction to Quantum Computation and Information*. Singapore: World Scientific.
- [48] Clauser, J. F., Horne, M. A., Shimony, A. y Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23(15), 880-884.
- [49] Aspect, A., Grangier, P. y Roger, G. (1982). Experimental realization of Einstein-Podolsky-Rosen-Bohm *Gedankenexperiment*: A new violation of Bell's inequalities. *Phys. Rev. Lett.*, 49(2), 91-94.
- [50] Cuevas, A., Carvacho, G., Saavedra, G., Cariñe, J., Nogueira, W. A. T., Figueroa, M., Cabello, A., Mataloni, P., Lima, G. y Xavier, G. B. (2013). Long-distance distribution of genuine energy-time entanglement. *Nat Commun*, 4, 1-6.
- [51] Boschi, D., Branca, S., De Martini, F., Hardy, L. y Popescu, S. (1998). Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 80(6), 1121-1125.
- [52] Tittel, W., Brendel, J., Gisin, B., Herzog, T., Zbinden, H. y Gisin, N. (1998). Experimental demonstration of quantum correlations over more than 10 km. *Phys. Rev. A*, 57(5), 3229-3232.
- [53] Hagley, E., Maître, X., Nogue, G., Wunderlich, C., Brune, M., Raimond, J. M. y Haroche, S. (1997). Generation of Einstein-Podolsky-Rosen pairs of atoms. *Phys. Rev. Lett.*, 79(1), 1-5.
- [54] Apostol, T. M. (2002). *Calculus: Tomo 2* (2a. ed.). Barcelona, España: Editorial Reverté, S. A.

Apéndice A

Desigualdades de Bell y CHSH

Este apéndice está basado en [11].

La desigualdad de Bell [29] se puede obtener considerando la existencia de un sistema físico compuesto por dos subsistemas A y B , el que es descrito por un conjunto de variables ocultas λ . Se considera que el sistema está compuesto de dos partículas de espín $\frac{1}{2}$ y que se mide en un experimento $\sigma_{\vec{a}}^A$ en la dirección \vec{a} y $\sigma_{\vec{b}}^B$ en la dirección \vec{b} .

Los posibles resultados serán:

$$\sigma_{\vec{a}}^A \longrightarrow A(\vec{a}, \lambda) = \pm 1, \quad (\text{A0.1})$$

$$\sigma_{\vec{b}}^B \longrightarrow B(\vec{b}, \lambda) = \pm 1, \quad (\text{A0.2})$$

donde \vec{a} y \vec{b} son vectores unitarios. Además, existe una anticorrelación perfecta si se mide en la misma dirección, esto es, $A(\vec{a}, \lambda)B(\vec{a}, \lambda) = -1$, lo cual implica que las partículas de espín están en sentido opuesto. Los resultados que se obtiene de cada subsistema se multiplican entre sí, repitiendo el experimento varias veces, de modo que el promedio de estas mediciones será

$$E(\vec{a}, \vec{b}) = \int d\lambda \rho(\lambda) A(\vec{a}, \lambda) B(\vec{b}, \lambda), \quad (\text{A0.3})$$

donde $\rho(\lambda) \geq 0$ corresponde a la distribución estadística de las variables ocultas que satisfacen la relación $\int d\lambda \rho(\lambda) = 1$.

Supóngase que la partícula se mide en una dirección adicional \vec{c} , se puede establecer

una diferencia entre las mediciones realizadas en las distintas direcciones,

$$E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c}) = d\lambda\rho(\lambda)A(\vec{a}, \lambda)\left[B(\vec{b}, \lambda) - B(\vec{c}, \lambda)\right]. \quad (\text{A0.4})$$

Utilizando la propiedad de anticorrelación y dado que $A^2 = 1$, se tiene,

$$E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c}) = -d\lambda\rho(\lambda)A(\vec{a}, \lambda)A(\vec{a}, \lambda)\left[1 + A(\vec{b}, \lambda)B(\vec{c}, \lambda)\right], \quad (\text{A0.5})$$

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

$$E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c}) \geq -d\lambda\rho(\lambda)\left[1 + A(\vec{b}, \lambda)B(\vec{c}, \lambda)\right] = -1 - E(\vec{b}, \vec{c}). \quad (\text{A0.6})$$

Análogamente, para el caso del mínimo valor $A(\vec{a}, \lambda)A(\vec{b}, \lambda) = -1$ se tiene que

$$E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c}) \leq d\lambda\rho(\lambda)\left[1 + A(\vec{b}, \lambda)B(\vec{c}, \lambda)\right] = 1 + E(\vec{b}, \vec{c}). \quad (\text{A0.7})$$

De esta forma, la desigualdad de Bell toma la forma

$$\left|E(\vec{a}, \vec{b}) - E(\vec{a}, \vec{c})\right| \leq -1 + E(\vec{b}, \vec{c}), \quad (\text{A0.8})$$

la cual depende solo de los ángulos de las distintas direcciones de medida y que se debe satisfacer si la teoría de variables ocultas es válida. Sin embargo, si se considera el estado singlete para dos partículas de espín $\frac{1}{2}$,

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|\uparrow_a\rangle|\downarrow_B\rangle - |\downarrow_A\rangle|\uparrow_B\rangle), \quad (\text{A0.9})$$

que corresponde a un estado maximalmente entrelazado, no se satisface la desigualdad (A0.8) en consecuencia, la teoría de las variables ocultas no puede ser correcta.

Además, si uno de los observadores mide en las direcciones \vec{a} y \vec{b} , y otro observador mide en las direcciones \vec{c} y \vec{d} , se tiene una desigualdad de Bell generalizada conocida como desigualdad de Clauser-Horne-Shimony-Hold (CHSH) [48],

$$|S| = |\langle ac\rangle - \langle ad\rangle + \langle bc\rangle + \langle bd\rangle| \leq 2. \quad (\text{A0.10})$$

La desigualdad de CSH fue comprobada experimentalmente [49], utilizando pares de fotones entrelazados en polarización. Además, en el 2013 un artículo ratifica experimentalmente la quebrantación de la desigualdad de Bell y su respectiva generalización para estados entrelazados [50].

Adicionalmente, se han reportado en la literatura correlaciones no locales en experimentos realizados con fotones entrelazados [51, 52] y con pares de átomos entrelazados [53], por lo tanto, los resultados experimentales se ajustan a las predicciones de la mecánica cuántica y no a las predicciones de una teoría local (de variables ocultas).



Apéndice B

Esquema de Extracción de Entrelazamiento Determinista

La correlaciones en los estados bipartitos $|\psi_{\theta,\phi}\rangle$ y $|\psi_{\theta+\pi,\phi}\rangle$ están caracterizadas por las concurrencias $C_{\theta,\phi}$ y $C_{\theta+\pi,\phi}$. El entrelazamiento promedio,

$$\bar{C}(\theta, \phi) = P_{\theta,\phi}C_{\theta,\phi} + P_{\theta+\pi,\phi}C_{\theta+\pi,\phi}, \quad (\text{B0.1})$$

almacenado en el sistema de dos qubits restante, varía entre los valores máximo y mínimo,

$$\bar{C}_{\text{mín}} = \min_{\{\theta,\phi\}} \{\bar{C}(\theta, \phi)\}, \quad (\text{B0.2})$$

$$\bar{C}_{\text{máx}} = \max_{\{\theta,\phi\}} \{\bar{C}(\theta, \phi)\}. \quad (\text{B0.3})$$

El escenario determinista corresponde al caso cuando ambos resultados, $|\psi_{\theta,\phi}\rangle$ y $|\psi_{\theta+\pi,\phi}\rangle$, tienen el mismo valor de concurrencia,

$$C_d = \underset{\theta_d, \phi_d}{\text{find}} \{C_{\theta_d, \phi_d} = C_{\theta_d + \pi, \phi_d}\}, \quad (\text{B0.4})$$

en este caso $\bar{C}(\theta_d, \phi_d) = C_d$. La situación cuando $C_d > C_{23}$ es una mejora determinista del entrelazamiento del sistema de dos qubits (estado puro). Resulta que el valor C_d está directamente relacionado a $\bar{C}_{\text{mín}}$ y $\bar{C}_{\text{máx}}$, como se demuestra en los siguientes teoremas.

En lo que sigue y sin pérdida de generalidad, se consideran estados puros de tres qubits con coeficientes reales,

$$|\psi\rangle = \sum_{p,q,r=0}^1 c_{pqr} |pqr\rangle, \quad (\text{B0.5})$$

con $c_{pqr} = c_{pqr}^*$ y $\sum c_{pqr}^2 = 1$.

Teorema I. $\bar{C}_{\text{mín}}$ y $\bar{C}_{\text{máx}}$ son funciones por partes de los parámetros de estado,

$$\begin{aligned} \bar{C}_{\text{mín}} &= \text{mín} \left\{ \sqrt{X_y^2 + X_z^2}, |X_x| \right\}, \\ \bar{C}_{\text{máx}} &= \text{máx} \left\{ \sqrt{X_y^2 + X_z^2}, |X_x| \right\}, \end{aligned} \quad (\text{B0.6})$$

donde las funciones X_j , $j = x, y, z$ dependientes del estado están definidas como

$$X_j = \langle \psi | \hat{\delta}_j \otimes \hat{\sigma}_y \otimes \hat{\sigma}_y | \psi \rangle. \quad (\text{B0.7})$$

El caso $\bar{C}_{\text{mín}} = \bar{C}_{\text{máx}}$ ocurre cuando $X_y = 0$ y $|X_x| = |X_z|$ o $|X_x| = \sqrt{X_y^2 + X_z^2}$, lo que corresponde a los estados dados por (B0.5) con *three-tangle* nulo, $\tau = 0$.

Teorema II. Los valores extremos de la concurrencia determinista C_d coinciden con $\bar{C}_{\text{máx}}$ y $\bar{C}_{\text{mín}}$, donde

a) el valor $\sqrt{X_y^2 + X_z^2}$ es obtenido proyectando en la base

$$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle - i|1\rangle}{\sqrt{2}}. \quad (\text{B0.8})$$

b) el valor $|X_x|$ puede ser conseguido proyectando en las bases

$$|\theta_d, \phi_d\rangle, |\theta_d + \pi, \phi_d\rangle \quad \text{o} \quad |\theta_d - \pi/2, \phi_d\rangle, |\theta_d + \pi/2, \phi_d\rangle \quad (\text{B0.9})$$

$$\theta_d = \arctan\left(\frac{X_x Y_z - X_z}{X_x Y_x - X_y}\right), \quad \phi_d = \pi, \quad (\text{B0.10})$$

donde $Y_j = \langle \psi | \hat{\sigma}_j \otimes \hat{I} \otimes \hat{I} | \psi \rangle$, $j = x, y, z$.

Estos teoremas proveen un protocolo experimentalmente realizable para una extracción determinista del entrelazamiento bipartito máximo posible desde un estado tripartito puro: primero, para un estado dado, se determina

máx $\{\sqrt{X_y^2 + X_z^2}, |X_x|\}$ y luego se mide el primer qubit en la base apropiada, ya sea (B0.8) o (B0.9).



Apéndice C

Método de multiplicadores de Lagrange

Una herramienta poderosa cuando se necesita extremizar una función de varias variables sujeta a una o más restricciones es el método de los multiplicadores de Lagrange [54].

Si una función $f(x_1, \dots, x_n)$ tiene un extremo relativo cuando está sometida a m restricciones:

$$\begin{aligned} g_1(x_1, \dots, x_n) &= 0, \\ &\vdots \\ g_m(x_1, \dots, x_n) &= 0, \end{aligned} \tag{C0.1}$$

siendo $m < n$, entonces existen m escalares $\lambda_1, \dots, \lambda_m$ tales que

$$\nabla f = \lambda_1 \nabla g_1 + \dots + \lambda_m \nabla g_m \tag{C0.2}$$

en cada punto extremo.

En la práctica, para encontrar los puntos que extremizan la función f , se considera el sistema de $n + m$ ecuaciones formado por las m ecuaciones de restricción (C0.1) más las n ecuaciones determinadas por la relación vectorial (C0.2). Se resuelve el sistema respecto a las $n + m$ incógnitas x_1, \dots, x_n y $\lambda_1, \dots, \lambda_m$. Los puntos (x_1, \dots, x_n) en los que se presentan los extremos relativos se encuentran entre las

soluciones del sistema.

Los escalares $\lambda_1, \dots, \lambda_m$ se denominan *multiplicadores de Lagrange*. Se introduce un multiplicador por cada restricción. La función f y las funciones de restricción g_1, \dots, g_m se suponen diferenciables.

