Computación Cuántica

Alan Boette
Raúl Rossignoli

Universidad Nacional de La Plata
2025

Estas notas se basan en los cursos dictados en la *Universidad Nacional de La Plata*:

- Introducción a a Arquitectura de Computadoras Cuánticas (Facultad de Ingeniería)
- Teoría de la Información Cuántica (Facultad de Ciencias Exactas)

Actualmente se trata de una versión preliminar por lo que pueden haber errores, partes incompletas o por mejorar. Cualquier tipo de sugerencia en este sentido, es bienvenida.

Agradecemos particularmente a Paula Pagano que colaboró con notas del curso, a Mauricio Matera y a Norma Canosa.

Índice general

1 Introducción

1.1. Mecánica Cuántica

La mecánica cuántica es, en resumen, la teoría que describe el funcionamiento de todo el universo, pero que solo se manifiesta en forma directa en ciertos regímenes donde los efectos "clásicos"son menos relevantes (es decir, a pequeñas longitudes, bajas temperaturas, bajas energías, altas presiones, etc.). Esta teoría presenta varias ideas poco intuitivas pero sin embargo, describe con perfecta precisión numerosos fenómenos que observamos experimentalmente a nivel microscópico.

En el último tiempo ha habido un crecimiento exponencial en el interés en la teoría de la información cuántica y computación cuántica. Numerosas organizaciones gubernamentales y privadas (Google, IBM, Nasa, D-Wave, Microsoft, Russian Quantum Center, Chinese Academy of Sciences, European Flagship Initiative on Quantum Technology, etc.) han estado invirtiendo cifras exorbitantes impulsando la "carrera" en búsqueda de la computadora cuántica.

Lo que a principios de los años ochenta surgía como la idea "peculiar" de utilizar sistemas cuánticos para realizar una tarea en forma más eficiente que cualquier algoritmo clásico [8], hoy claramente se ve como un incipiente cambio de paradigma tecnológico. Entre los algoritmos más notables que surgieron inicialmente, se pueden mencionar el de factorización de Shor [9], que logra una reducción exponencial en el número de pasos requeridos, y el algoritmo cuántico de búsqueda de Grover [10], que mostraron el potencial de una computación basada en la mecánica cuántica (qubits en lugar de bits [11]). Puede mencionarse también el algoritmo de muestreo bosónico (boson sampling) de Arhikonov [12], que también logra una reducción exponencial. El protocolo de teleportación cuántica [13] demostró que la mecánica cuántica podía también utilizarse para generar nuevas formas de transmisión de información. Hoy en día son innumerables los desarrollos que se hacen continuamente, tanto a nivel teórico, experimental como incluso a través de la fabricación de dispositivos (como ejemplo de criptografía cuántica: en 2016 China lanzó el satélite QUESS: Quantum Experiments at Space Scale, capaz de recibir y transmitir claves encriptadas).

Entre las características de los sistemas cuánticos que hacen posible estos avances sobresale el entrelazamiento cuántico, término establecido por Edwin Schrödinger en 1935 [14] para referirse a la capacidad de sistemas cuánticos compuestos de exhibir correlaciones entre sus componentes sin análogo clásico.

La determinación exacta del entrelazamiento entre las distintas partes de un sistema compuesto en interacción, es un problema extraordinariamente difícil ya que requiere recursos que crecen exponencialmente con el número de componentes.

En estas notas del Curso Teoría de la Información Cuántica, cubriremos los contenidos básicos necesarios para comprender la teoría y los algoritmos de la computación cuántica.

1.2. Notación de Dirac

Es importante señalar que el formalismo de la mecánica cuántica se basa en el del álgebra lineal, por este motivo es útil introducir algunos conceptos básicos. Tanto en Mecánica Cuántica como especialmente en Computación Cuántica se emplea la notación de "bra-ket" introducida por Dirac.

Es decir, introducimos dos definiciones: el "bra" y el "ket" que al calcular un producto interno (ver Sección 1.3), forman un "bra-ket"(bracket es corchete en inglés).

Expresado en forma simple, el ket, escrito como $|\psi\rangle$, donde ψ es una variable arbitraria usada para etiquetar al ket, representa un vector columna de longitud arbitraria. El bra, $\langle\psi|$ representa su transpuesto conjugado. Para un ejemplo de 2 por 1, el ket $|\psi\rangle$ es tal que

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \quad \langle\psi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}.$$

En general, $|\psi\rangle$ es un vector en un espacio vectorial complejo con producto interno, denominado espacio de Hilbert $\mathcal{H}$ (o espacio de estados), mientras que $\langle\psi|$ es un vector del espacio dual asociado $\mathcal{H}^*$, tal que $\langle\phi|\psi\rangle$ es el producto interno entre $|\phi\rangle$ y $|\psi\rangle$. En información cuántica se suelen emplear espacios de dimensión finita n, tal que $\mathcal{H} = \mathbb{C}^n$, que corresponden a subespacios de un espacio de Hilbert de dimensión infinita.

1.3. Producto Interno

Es necesario subrayar ciertos conceptos para aplicar álgebra lineal en mecánica cuántica. En primer lugar el concepto de producto interno usando notación de Dirac.

En realidad la notación de Dirac permite que el producto interno se calcule de forma sencilla. Por ejemplo, para calcular el producto de $|\psi\rangle$ con sí mismo, simplemente se multiplica por su transpuesto conjugado, que es justamente $\langle\psi|$. Por lo que queda: $\langle\psi|\psi\rangle$. Para un estado normalizado $\langle\psi|\psi\rangle = 1$.

Tomando $|\psi\rangle$ perteneciente a $\mathbb{C}^{\mathrm{n}}$, se puede representar $|\psi\rangle$ como una superposición de los elementos de una base ortonormal $\{|e_i\rangle\ ,\ i = 1, \ldots, n,\ \langle e_i|e_j\rangle = \delta_{ij}\}$ de $\mathbb{C}^{\mathrm{n}}$:

$$|\psi\rangle = \sum_{i=1}^{\mathrm{n}} \alpha_i |e_i\rangle$$

para $\alpha_i \in \mathbb{C}$, con $\langle\psi| = \sum_{i=1}^{n} \alpha_i^* \langle e_i|$. Para un estado normalizado,

$$\langle\psi|\psi\rangle = \sum_{i,j=1}^{\mathrm{n}} \alpha_j^* \alpha_i \langle e_j|e_i\rangle = \sum_{i,j=1}^{\mathrm{n}} \alpha_j^* \alpha_i \delta_{ij} = \sum_{i=1}^{\mathrm{n}} \alpha_i^* \alpha_i = \sum_{i=1}^{\mathrm{n}} |\alpha_i|^2 = 1$$

El producto interno ("overlap") entre dos estados diferentes $|\psi\rangle$ y $|\phi\rangle = \sum_{i=1}^{n} \beta_i |e_i\rangle$ es

$$\langle\phi|\psi\rangle = \sum_{i=1}^{n} \beta_i^* \alpha_i = \langle\psi|\phi\rangle^*$$

y es un concepto muy importante en mecánica cuántica. Para estados normalizados su módulo $|\langle\phi|\psi\rangle|$ está comprendido entre 0 y 1.

2 Postulados de la Mecánica Cuántica

> "On ne voit bien qu'avec le coeur. L'essentiel est invisible pour les yeux."
>
> *Antoine de Saint-Exupéry*

2.1. Espacio de un Estado Físico

Postulado 1. *A todo sistema físico aislado se le asigna un espacio vectorial complejo dotado de producto interno, es decir, un espacio de Hilbert, el cual se conoce como* espacio del estado *de un sistema. Dicho sistema se describe completamente por un vector unitario que vive en este espacio, llamado* vector estado.

El sistema mecánico cuántico más simple y el de mayor aplicación en este contexto es el *qubit*. Un qubit vive un espacio de dos dimensiones. Supongamos que $|0\rangle$ y $|1\rangle$ forman un base ortonormal de este espacio. Luego un vector estado arbitrario se puede escribir como

$$|\psi\rangle = a|0\rangle + b|1\rangle,$$

donde a y b son números complejos. La condición de que $|\psi\rangle$ sea unitario, $\langle\psi|\psi\rangle = 1$, se la conoce comúnmente como la *condición de normalización* para vectores estado y es imprescindible para que los vectores describan estados físicos. Para el caso del qubit, es entonces equivalente a $|a|^2 + |b|^2 = 1$.

Superposición. Decimos que cualquier combinación lineal $\sum_i \alpha_i|\psi_i\rangle$ es una *superposición* de los estados $|\psi_i\rangle$ con *amplitud* α_i para el estado $|\psi_i\rangle$.

2.2. Evolución

Postulado 2. *La evolución de un sistema cuántico* cerrado *se describe por una* transformación unitaria. *Esto es, el estado $|\psi(t_1)\rangle$ del sistema al tiempo t_1 esta relacionado con el estado*

del sistema $|\psi(t_2)\rangle$ *al tiempo* t_2 *a través de un operador unitario* U *que depende solo de los tiempos* t_1 *y* t_2*,*

$$|\psi(t_2)\rangle = U|\psi(t_1)\rangle.$$

De forma equivalente, la evolución de un estado de un sistema cuántico cerrado *también se describe por* la ecuación de Schrödinger*,*

$$i\hbar\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = H|\psi\rangle. \tag{2.1}$$

En la ecuación de Schrödinger, $\hbar = \frac{h}{2\pi}$ se denomina textith partida, donde h es una constante física conocida como la *constante de Planck* cuyo valor se debe determinar experimentalmente. El valor exacto no de relevancia en este contexto por lo que en la práctica es común absorber el factor $\hbar$ dentro de H, fijando de forma efectiva $\hbar = 1$. H es un operador hermítico fijo conocido como el *Hamiltoniano* del sistema cerrado.

Dado que el Hamiltoniano es un operador hermítico tiene una descomposición espectral

$$H = \sum_E E|E\rangle\langle E|, \tag{2.2}$$

con autovalores E y sus correspondientes autovectores normalizados $|E\rangle$. Los estados $|E\rangle$ convencionalmente se los llama *autoestados de energía*, o a veces *estados estacionarios*, y E es la *energía* del estado $|E\rangle$. A la energía más baja se conoce como el *estado fundamental de energía* del sistema, y al correspondiente autovalor (o autoespacio) de energía se lo conoce como el *estado fundamental*. El motivo por el que en ciertas ocasiones se conoce a los estados $|E\rangle$ como estados estacionarios es porque su único cambio con el tiempo es adquirir un factor numérico global,

$$|E\rangle \to \exp(-iEt/\hbar)|E\rangle.$$

La solución a la ecuación de Schödinger's es:

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]|\psi(t_1)\rangle = U(t_1,t_2)|\psi(t_1)\rangle,$$

donde definimos

$$U(t_1,t_2) \equiv \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]. \tag{2.3}$$

La ecuación 2.3 refleja la equivalencia entre las dos descripciones de evolución.

[11] Ejercicio 2.54: Suponer que A y B son operadores hermíticos conmutantes. Probar que $\exp(A)\exp(B) = \exp(A+B)$.

SOLUCIÓN: Dado que A y B conmutan, se pueden diagonalizar simultáneamente. Escribimos $A = \sum_i a_i|i\rangle\langle i|$, $B = \sum_j b_j|j\rangle\langle j|$, notando que $A + B = \sum_i (a_i + b_i)|i\rangle\langle i|$. Luego, $\exp(A) = \sum_i e^{a_i}|i\rangle\langle i|$, $\exp(B) = \sum_j e^{b_j}|j\rangle\langle j|$, $\exp(A+B) = \sum_i e^{a_i+b_i}|i\rangle\langle i|$. Es claro que

$$\begin{aligned}\exp(A)\exp(B) &= \left(\sum_i e^{a_i}|i\rangle\langle i|\right)\left(\sum_j e^{b_j}|j\rangle\langle j|\right) \\ &= \sum_{i,j} e^{a_i}e^{b_j}|i\rangle\delta_{ij}\langle j| \\ &= \sum_i e^{a_i}e^{b_i}|i\rangle\langle i| \\ &= \sum_i e^{a_i+b_i}|i\rangle\langle i| = \exp(A+B),\end{aligned}$$

lo cual prueba el resultado.

2.3. Medida en Mecánica Cuántica

Postulado 3. *Las medidas en Mecánica Cuántica se describen por un conjunto de* operadores de medida*: $\{M_m\}$. Estos operadores actúan sobre el estado $|\psi\rangle$ y el índice m hace referencia a la salida del experimento. El estado del sistema después de la medida es*

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

y la probabilidad de obtener el resultado m está dada por

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle.$$

Los operadores de medida satisfacen la ecuación de completitud*,*

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

La ecuación de completitud expresa el hecho de que la probabilidades suman uno:

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

A su vez, queda claro que la condición de normalización para estados físicos es imprescindible para que las probabilidades esten bien definidas.

2.4. Distinguiendo estados cuánticos

Es más simple comprender la distinguibilidad de estados a través de un juego que involucra dos partes, Alice y Bob. Alice elige estados $|\psi_i\rangle (1 \leq i \leq n)$ a partir de un conjunto fijo de estados conocidos para ambos. Ella le da el estado $|\psi_i\rangle$ a Bob, que tiene la tarea de identificar el índice i de el estado que Alice le dió.

Supongamos que los estados $|\psi_i\rangle$ son ortonormales. Luego Bob puede hacer una medida cuántica para distinguir los estados, utilizando el siguiente procedimiento. Define los operadores de medida $M_i \equiv |\psi_i\rangle\langle\psi_i|$, asignando uno a cada índice i, y un operador de medida adicional M_0 definido como la raíz cuadrad positiva del operador $I - \sum_{i\neq 0}|\psi_i\rangle\langle\psi_i|$. Estos operadores satisfacen la relación de completitud, y si el estado $|\psi_i\rangle$ es preparado entonces $p(i) = \langle\psi_i|M_i|\psi_i\rangle = 1$, por lo que el resultado i ocurre con certeza. Luego, es posible distinguir los estados ortonormales $|\psi_i\rangle$.

Por otro lado, si los estados $|\psi_i\rangle$ no son ortonormales podemos entonces demostrar que no existe *medida cuántica capaz de distinguir a los estados*.

Teorema 1. *Los estados no ortogonales no se pueden distinguir de manera confiable a través de medidas.*

Demostración. Una demostración por el absurdo muestra que no existe una medida que distinga estados no-ortogonales $|\psi_1\rangle$ y $|\psi_2\rangle$. Supongamos que dicha medida sí es posible: Si se prepara el estado $|\psi_1\rangle$ ($|\psi_2\rangle$), luego la probabilidad de medir j tal que $f(j) = 1$ ($f(j) = 2$) debe ser 1. Definiendo $E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$, estas observaciones se pueden escribir como:

$$\langle\psi_1|E_1|\psi_1\rangle = 1; \langle\psi_2|E_2|\psi_2\rangle = 1.$$

Dado que $\sum_i E_i = I$ se ve que $\sum_i\langle\psi_1|E_i|\psi_1\rangle = 1$, y dado que $\langle\psi_1|E_1|\psi_1\rangle = 1$, se debe tener $\langle\psi_1|E_2|\psi_1\rangle = 0$, por lo que $\sqrt{E_2}|\psi_1\rangle = 0$. Supongamos que descomponemos $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\phi\rangle$, donde $|\phi\rangle$ es ortonormal a $|\psi_1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, y $|\beta| < 1$ dado que $|\psi_1\rangle$ y $|\psi_2\rangle$ no son ortogonales. Entonces $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\phi\rangle$, lo que implica una contradicción, ya que

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\langle\phi|E_2|\phi\rangle \leq |\beta|^2 < 1,$$

donde la última desigualdad surge de la observación de que

$$\langle\phi|E_2|\phi\rangle \leq \sum_i \langle\phi|E_i|\phi\rangle = \langle\phi|\phi\rangle = 1.$$

□

2.5. Medidas Proyectivas

Medidas Proyectivas. Una medida proyectiva está descripta por un *observable*, M, un operador hermítico que actúa sobre el estado del sistema. Este tiene una descomposición espectral

$$M = \sum_m mP_m,$$

donde P_m es un proyector en el autoespacio de M con autovalor m. Las posibles salidas de la medida corresponden a los autovalores, m, de este observable. Midiendo al estado $|\psi\rangle$, la probabilidad de obtener el resultado m está dada por $p(m) = \langle\psi|P_m|\psi\rangle$. Si se obtiene el resultado m, el estado del sistema luego de la medida es

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

Las medidas proyectivas son un caso especial en el que los operadores M_m definidos en el Postulado 3, además de satisfacer la relación $\sum_m M_m^\dagger M_m = I$, son proyectores ortogonales, es decir, M_m son hermíticos y $M_m M_{m'} = \delta_{m,m'} M_m$.

El promedio de una medida es

$$\begin{aligned}\langle M\rangle &= \sum_m mp(m)\\ &= \sum_m m\langle\psi|P_m|\psi\rangle\\ &= \langle\psi|\left(\sum_m mP_m\right)|\psi\rangle\\ &= \langle\psi|M|\psi\rangle;\end{aligned}$$

el valor promedio de un observable M comúnmente se escribe como $\langle M\rangle \equiv \langle\psi|M|\psi\rangle$. A partir de esta formula para los promedios se obtiene una expresión para la desviación estándar asociada a la observación de M,

$$[\Delta(M)]^2 = \langle(M - \langle M\rangle)^2\rangle = \langle M^2\rangle - \langle M\rangle^2.$$

2.5.1. Medidas POVM

Positive Operator-Valued Measure (POVM). Supongamos que se realiza una medida sobre un sistema cuántico en el estado $|\psi\rangle$ descripta por operadores de medida M_m. Luego la probabilidad de obtener el resultado m está dada por $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Si definimos

$$E_m \equiv M_m^\dagger M_m.$$

Luego, a partir del Postulado 3 y operaciones de álgebra lineal, se ve que E_m es un operador positivo tal que $\sum_m E_m = I$ y $p(m) = \langle\psi|E_m|\psi\rangle$. Luego el conjunto de operadores E_m permite determinar las probabilidades de diferentes resultados de medida. A los operadores E_m se los conoce como *elementos POVM* asociados a la medida. Al conjunto completo de los $\{E_m\}$ se los llama *POVM*.

3 Fundamentos:

3.1. El Qubit: Quantum Bit

Un bit cuántico (*qubit*) se describe por un *estado* de dimensión 2. Un bit clásico puede solo tomar valores 0 o 1. De igual forma un qubit puede estar en el estado $|0\rangle$ o $|1\rangle$, que corresponden a los estados de un bit clásico 0 y 1. La diferencia entre un bit y un qubit, es que el qubit puede estar en una *superposición* de $|0\rangle$ y $|1\rangle$ al mismo tiempo. Este fenómeno se lo puede observar tanto en el espín de un electrón como en la polarización de un fotón. El estado de un qubit se puede describir de la siguiente manera:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{3.1}$$

donde α y β son números complejos. Aquí α y β son las *amplitudes de probabilidad*, y $|0\rangle$, $|1\rangle$ se denominan estados de la *base estándar computacional*.

Las amplitudes de un qubit no se pueden determinar directamente, es necesario medirlo. Si lo medimos, podemos obtener $|0\rangle$ con probabilidad $|\alpha|^2$, o $|1\rangle$ con probabilidad $|\beta|^2$. La suma de los valores absolutos al cuadrado de las amplitudes siempre suman 1 por el hecho de tratarse de probabilidades. Esto está garantizado por la condición de normalización de los estados físicos, anteriormente mencionada ($|\alpha|^2 + |\beta|^2 = 1$).

Por ejemplo midiendo al qubit en el estado

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3.2}$$

se obtiene $|0\rangle$ la mitad de las veces y $|1\rangle$ la otra mitad ($|1/\sqrt{2}|^2 = 0.5$). Este estado se lo denota $|+\rangle$.

3.1.1. La Esfera de Bloch

La esfera de Bloch es la representación geométrica del estado de un qubit. Es un sistema de coordenadas esféricas en el cual un estado cuántico se lo puede describir como

$$|\psi\rangle = e^{i\delta}\left(\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle\right), \tag{3.3}$$

donde δ, θ y ϕ son números reales. El factor $e^{i\delta}$ es una fase global del estado. Este factor no influye en las probabilidades de medida, ya que $\left|e^{i\delta}\right| = 1$, por lo que es usual omitirlo, permitiéndonos escribir

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle. \tag{3.4}$$

Los números θ y ϕ definen un punto en la esfera tridimensional (Figure 3.1). La esfera de Bloch es muy útil para visualizar operaciones de un qubit. Sin embargo, existen limitaciones para generalizar la esfera de Bloch a muchos qubits.

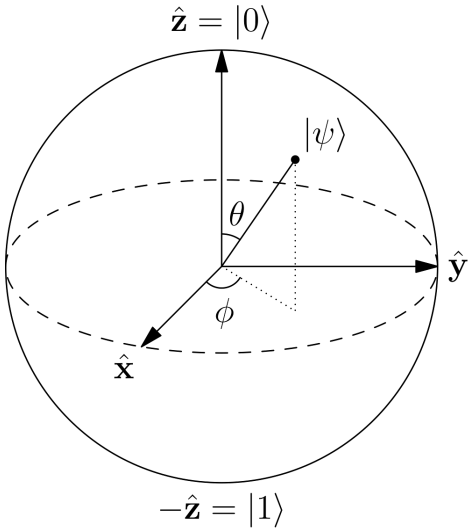
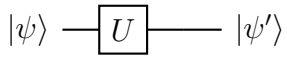


Figura 3.1: Representación de un qubit en la esfera de Bloch.

3.1.2. Compuertas de un qubit: Single-Qubit Gates

Las compuertas de un qubit se pueden ver como rotaciones en la esfera de Bloch. Estas compuertas son *unitarias*, es decir $U^\dagger U = UU^\dagger = I$, donde $U^\dagger$ es la transpuesta conjugada de U y I la identidad. Por lo que cualquier unitaria de $2^n \times 2^n$ es una compuerta válida que actúa en n qubits. Comúnmente $|\psi'\rangle = U|\psi\rangle$ se representan a través un circuito:



A continuación se describen y visualizan algunas compuertas de un qubit usuales.

3.1.3. Compuertas de Pauli

Las compuertas de un qubit más simples son las matrices de *Pauli:* I, X, Y y Z. Donde I es la identidad y las compuertas X, Y y Z rotan π radianes alrededor de los ejes X, Y o Z, respectivamente.

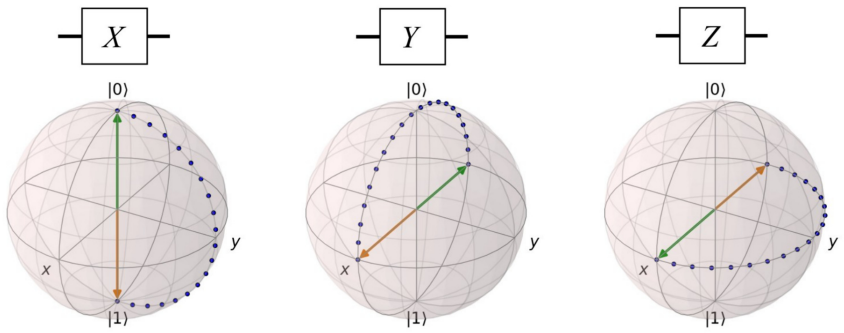


Figura 3.2: Compuertas X, Y y Z visualizadas en la esfera de Bloch. El vector inicial está en verde y el naranja es el de la posición final.

3.1.4. Compuerta Hadamard

La compuerta *Hadamard* (H) (Figura 3.3) mapea los estados de la base estándar $|0\rangle$ y $|1\rangle$ a estados de superposición con pesos iguales:

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle \tag{3.5}$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle. \tag{3.6}$$

Es la combinación de dos rotaciones de π alrededor del eje Z seguidas de una $\pi/2$ alrededor del eje. También se la puede ver como una rotación de π alrededor del eje $n = (1, 0, 1)/\sqrt{2}$.

3.1.5. Compuerta Fase

Compuertas de que rotan alrededor del eje Z se llaman *Compuertas Fase*. Rotan la fase del estado $|1\rangle$ un ángulo θ dejando igual al estado $|0\rangle$:

$$\begin{aligned} R_z(\theta)|0\rangle &= |0\rangle \\ R_z(\theta)|1\rangle &= e^{i\theta}|1\rangle. \end{aligned} \tag{3.7}$$

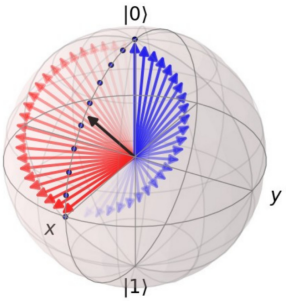


Figura 3.3: Visualización de la compuerta Hadamard en la esfera de Bloch.

La probabilidad de medir $|0\rangle$ o $|1\rangle$ no cambia al aplicar la compuerta fase, como su nombre lo indica solo cambia la fase del estado cuántico. Una compuerta fase común es la compuerta S, donde $\theta = \pi/2$ (Figure 3.4). La compuerta Pauli Z se puede pensar como una compuerta fase con $\theta = \pi$ (dado que $e^{i\pi} = -1$). Por lo que se puede pensar a la compuerta S como la mitad de la compuerta Z. Otra compuerta fase conocida es la compuerta T, donde $\theta = \pi/4$ (la mitad de una compuerta S).

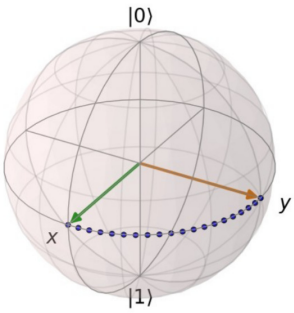


Figura 3.4: Visualización de la compuerta S en la esfera de Bloch.

3.1.6. Medida de un qubit

En la sección (2.3) se introdujo la idea de medida en mecánica cuántica, aquí vemos su aplicación más simple que es el caso de medir un qubit. Al medir un qubit $|\psi\rangle$ en la base computacional, la superposición cuántica colapsa a un estado de la base. Se dice que estado $|\psi\rangle$ "colapsó", quedando en el estado$|0\rangle$ o $|1\rangle$. Se puede calcular la probabilidad de que se obtenga cierto resultado de la medida a través de las amplitudes de probabilidad:

$$P(|0\rangle) = |\alpha|^2 \tag{3.8}$$

$$P(|1\rangle) = |\beta|^2. \tag{3.9}$$

Esto se puede observar en el circuito simple de un qubit:

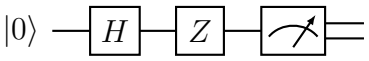


Figura 3.5: El resultado de la medida de un qubit es un bit clásico, que se diferencia de un qubit representándolo con un cable doble. Este circuito se puede visualizar en la esfera de Bloch en la Figura 3.6.

En primer lugar se calcula $H|0\rangle = |+\rangle$, seguido de $Z|+\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, (o $|-\rangle$). Finalmente se mide, obteniendo algún estado de la base computacional $|j\rangle$. Lo único que se puede afirmar es que se obtendrá el estado $|j\rangle$ con probabilidad $|a_j|^2$:

$$P(|0\rangle) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} \tag{3.10}$$

$$P(|1\rangle) = \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{1}{2}. \tag{3.11}$$

Teniendo igual probabilidad de medir $|0\rangle$ o $|1\rangle$.

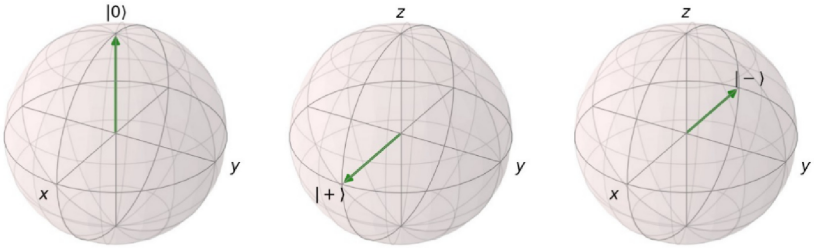


Figura 3.6: Estados del qubit a través del circuito: $|0\rangle \to H|0\rangle \to ZH|0\rangle$.

3.1.7. Notación Vectorial

Anteriormente vimos que un estado de un qubit se puede escribir como

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{3.12}$$

Los kets $|0\rangle$ y $|1\rangle$ forman la base estándar de un qubit y se representan como:

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}; \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}. \tag{3.13}$$

Como ya se mencionó un estado cuántico debe estar normalizado por lo que el estado de un qubit es un vector normalizado de un espacio vectorial complejo de dimensión 2. Un estado de n qubits tiene un *espacio de Hilbert* de dimensión 2^n. Un estado cuántico se puede escribir como combinación lineal de estados de la base:

$$|\psi\rangle = \alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\alpha\\\beta\end{pmatrix}. \tag{3.14}$$

Por lo que las compuertas de un qubit se pueden representar por matrices unitarias de 2×2:

$$I = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}; \qquad X = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}; \qquad Y = \begin{pmatrix}0 & -i\\i & 0\end{pmatrix};$$

$$Z = \begin{pmatrix}1 & 0\\0 & -1\end{pmatrix}; \qquad S = \begin{pmatrix}1 & 0\\0 & i\end{pmatrix}; \qquad H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}.$$

Luego, aplicar la compuerta X al estado $|0\rangle$, $X|0\rangle$ se puede calcular simplemente como una multiplicación de una matriz por un vector:

$$X|0\rangle = \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}. \tag{3.15}$$

Por lo que vemos que $X|0\rangle = |1\rangle$. De forma general:

$$X\begin{pmatrix}\alpha\\\beta\end{pmatrix} = \begin{pmatrix}\beta\\\alpha\end{pmatrix}. \tag{3.16}$$

Las compuertas cuánticas se pueden combinar multiplicando sus respectivas matrices. Por ejemplo, podemos verificar que la compuerta Hadamard es su propia inversa:

$$H^2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix} = I. \tag{3.17}$$

Es a su vez una *matriz Hermítica*, ya que es igual a su propia transpuesta conjugada: $H = H^\dagger$.

3.2. Multi-Qubits

Para representar más de un qubit se utiliza el *producto tensorial*. Dadas A una matriz de $m \times n$ y B una matriz de $p \times q$, luego

$$A \otimes B = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \dots & a_{mn}B \end{pmatrix}, \tag{3.18}$$

resultando en un matriz de $mp \times nq$. Se puede representar el estado de dos qubits $|00\rangle$ como

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ 0\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{3.19}$$

Las notaciones: $|00\rangle = |0\rangle|0\rangle = |0\rangle \otimes |0\rangle$, son equivalentes. El estado de dos qubits se puede escribir como:

$$|ab\rangle = |a\rangle \otimes |b\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{3.20}$$

Un estado en general se puede escribir como combinación lineal $\sum_j \alpha_j |\psi_j\rangle$ de estados $|\psi_j\rangle$ con sus amplitudes correspondientes α_j.

Notar que a diferencia de los bits clásicos, el espacio de un estado crece de forma exponencial con el número de qubits, con n qubits se pueden representar 2^n estados. Estados de muchos qubits, como cualquier estado cuántico tienen que estar normalizado. Para un estado de n qubits:

$$\sum_{j=0}^{2^n-1} |\alpha_j|^2 = 1. \tag{3.21}$$

3.2.1. Evolución de un estado de dos qubits

En la sección (2.2) se introdujo el concepto de evolución de un sistema cuántico cerrado, en esta sección veremos un ejemplo en el caso de dos qubits en el que la unitaria es simplemente aplicarle la compuerta H al segundo, $H_1|0_0 0_1\rangle$.Esto se puede obtener de forma simple:

$$H_1|0_0 0_1\rangle = (I_0 \otimes H_1)|0_0 0_1\rangle. \tag{3.22}$$

Si se quiere calcular la matriz explícitamente:

$$I_0 \otimes H_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.23}$$

$$= \frac{1}{\sqrt{2}} \left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right] \tag{3.24}$$

$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}. \tag{3.25}$$

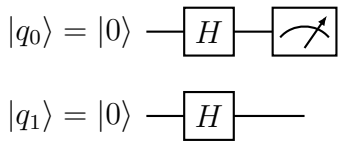
Por lo que vemos que $I_0 \otimes H_1|00\rangle$:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{3.26}$$

da como resultado el estado $(|00\rangle + |01\rangle)/\sqrt{2} = |0+\rangle$, como era de esperarse.

3.2.2. Medidas parciales de dos qubits

Ya se introdujo el concepto de medidas en la sección (2.3), en este caso vemos un ejemplo simple de dos qubits en el que se mide el qubit $|q_0\rangle$ como se observa en el circuito:



Inicialmente los dos qubits están en el estado $|00\rangle$ y se aplica la compuerta Hadamard a cada uno:

$$(H \otimes H)|00\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \tag{3.27}$$

si se mide el $|q_0\rangle$ se tiene mitad de probabilidad de obtener $|0\rangle$ o $|1\rangle$. Al medir, el estado $|q_0\rangle$ colapsa a alguno de los siguientes estados:

$$|\psi\rangle = \begin{cases} \frac{1}{\sqrt{2}}(|\underline{0}0\rangle + |\underline{0}1\rangle) \text{ if } M(q_0) = |0\rangle \\ \frac{1}{\sqrt{2}}(|\underline{1}0\rangle + |\underline{1}1\rangle) \text{ if } M(q_0) = |1\rangle \end{cases} \tag{3.28}$$

Luego de la medida se tienen dos estados posibles para $|q_0\rangle$: $|0\rangle$ o $|1\rangle$. El qubit $|q_1\rangle$ quedará en una superposición porque no se lo midió. Notar que los primeros qubits (subrayados) en ambos estados son iguales. Lo cual tiene sentido porque se midió este qubit por lo que se tiene certeza sobre este estado.

3.3. Compuertas de dos qubits usuales

3.3.1. Compuerta CNOT

La compuerta cuántica control-NOT (CNOT, a veces llamada control-X) es similar a la compuerta clásica XOR, pero es reversible. Esta compuerta tiene dos qubits de entrada el qubit de *control* y el qubit *target*. Si el qubit de control está en 0, luego se deja igual al qubit target. Pero si el qubit de control está en 1, el qubit target se invierte. El circuito que representa al CNOT se puede observar en la Figura 3.7. El qubit $|q_0\rangle$ representa al qubit de control y $|q_1\rangle$ representa al qubit target. Es esencialmente una compuerta X con un qubit de control. CNOT es hermítica.

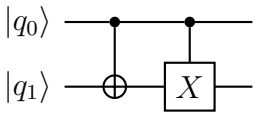
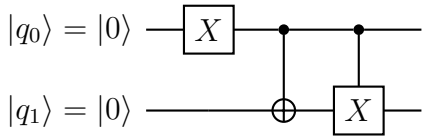


Figura 3.7: Dos formas diferentes de representar a CNOT en un circuito.

$$U_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Figura 3.8: Representación matricial de CNOT.

Veamos un ejemplo en el cual se utiliza la compuerta CNOT. Consideramos el siguiente circuito:



En primer lugar, se aplica X, para poner el qubit de control $|q_0\rangle$ en el estado $|1\rangle$, obteniendo el estado $|10\rangle$. Luego se aplica la compuerta CNOT,

$$\text{CNOT}|10\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle. \tag{3.29}$$

Dado que se puso el qubit de control en el estado $|1\rangle$, se invierte el qubit de target, obteniendo el estado $|11\rangle$.

3.3.2. Compuerta CZ

La compuerta CZ, o control-Z , actúa de forma similar a otras compuertas de control. Esto es, se aplica si el qubit de control está en $|1\rangle$ y en caso contrario no hace nada. En el caso de CZ la operación es la compuerta Z, la compuerta CZ también es hermítica.

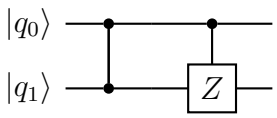


Figura 3.9: Dos formas diferentes de representar a CZ en un circuito.

3.3.3. Compuertas de Control

Las Compuertas de Control actúan en dos o más qubits, en las cuales uno o más qubits actúan como control para cierta operación. Generalmente, si U es una compuerta que opera sobre qubits individuales tiene una representación matricial:

$$U = \begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}, \tag{3.30}$$

luego la compuerta control-U en la que el qubit de control es el 0 y el target el 1, tiene la siguiente representación matricial:

$$C_U = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{pmatrix}. \tag{3.31}$$

3.4. Compuerta Toffoli

La compuerta Toffoli tiene tres entradas y salidas (Figura 3.10), donde dos de los qubits de entrada actúan como control. El tercer qubit es el target que se invierte cuando ambos qubits de control están en $|1\rangle$, en caso contrario no se le hace nada. Por ejemplo, si se aplica la compuerta Toffoli al estado $|110\rangle$, se invierte el tercer qubit, por lo que se obtiene el estado $|111\rangle$.

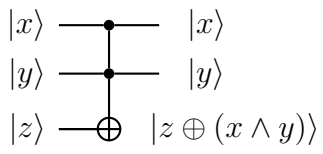


Figura 3.10: Circuito que representa la compuerta Toffoli, donde $\oplus$ es la suma binaria (XOR).

La compuerta Toffoli, o control-control-X (CCX) se puede representar por una matriz de 8×8:

$$U_{CCX} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}. \tag{3.32}$$

4 Entrelazamiento Cuántico

> " Solo sé que no sé nada y, al saber que nada sé,
> algo sé."
>
> *Sócrates*

Una propiedad clave que caracteriza el comportamiento de los sistemas en el régimen cuántico es el llamado *Entrelazamiento cuántico*. Esta propiedad puede entenderse como la imposibilidad de representar las correlaciones existentes en un sistema cuántico en términos de una distribución estadística sobre posibles configuraciones del sistema, especificables en términos de estados locales definidos. Para entender cómo esta noción es fundamental en la descripción clásica de los sistemas físicos, consideremos por ejemplo el sistema Tierra-Luna-Sol. Para la mecánica newtoniana, estos tres astros son entes distintos, con propiedades independientes. Así, en cada instante el Sol, la Tierra y la Luna cuentan con posiciones y velocidades bien definidas. El efecto de la interacción entre estos cuerpos se reduce entonces a cambiar las velocidades de estos cuerpos en función de las posiciones de los otros. Este marco de trabajo, que podemos llamar *reduccionista*, permite describir y predecir el comportamiento de la mayoría de los sistemas físicos macroscópicos en forma a la vez computacionalmente eficiente y precisa. Sin embargo, al tratar de aplicarlo a sistemas en la escala atómica comienza a mostrar sus fallas: en esta escala, el entrelazamiento implica que para ciertos estados del sistema, las propiedades de las partes no estén bien definidas. Por ejemplo, el estado típico de una molécula de Hidrógeno no puede en general describirse en términos de los estados de los átomos que la conforman: existen observables globales (la energía de la molécula, el impulso angular) que no son compatibles con los observables asociados a los átomos por separado. Esto nos obliga en mecánica cuántica a tratar los sistemas compuestos desde una perspectiva *holística*, en el sentido de que debemos tratar al sistema como un todo. Una consecuencia inmediata es que la descripción exacta de los sistemas cuánticos se vuelve mucho más compleja que la de su equivalente clásico.

Sin embargo, no todos los sistemas cuánticos parecen requerir de una descripción que aborde toda esa complejidad potencial. Por ejemplo, el sistema Tierra-Sol-Luna en sí es un sistema cuántico. La clave del éxito de su descripción clásica consiste en que en su evolución el estado de cada una de sus partes permanece bien definido. Decimos entonces que el sistema admite descripción en términos de *estados separables*. Por otro lado, la molécula de Hidrógeno típicamente se encuentra en un estado en el que el estado de sus partes

no está bien definido. Decimos por esto que su descripción requiere considerar *estados entrelazados*. Podemos decir entonces que cuanto más entrelazados se encuentren los estados típicos de un sistema (en un dado régimen) más nos costará representarlos en forma precisa y eficiente a la vez.

La definición y evaluación de medidas que cuantifiquen el grado de entrelazamiento presente en un sistema es una tarea bastante más compleja, tanto desde un punto de vista formal como práctico. En lo que resta del capítulo daremos una definición más formal de lo que es un *estado cuántico entrelazado* [11, 15-17]. Se introducirán entonces algunos elementos de la teoría de la información que nos permitirán definir medidas de entrelazamiento y de correlaciones cuánticas entre partes de un sistema.

4.1. Operador Densidad y Entropía de Von Neumann

El estado de un sistema cuántico se puede caracterizar por un *operador densidad* (o matriz densidad) ρ, el cual es un operador hermítico de traza 1 y con todos sus autovalores no negativos:

$$\rho \geq 0\,, \quad \mathrm{Tr}\rho = 1\,. \tag{4.1}$$

Este operador determina el valor medio de cualquier observable O:

$$\langle O \rangle = \mathrm{Tr}\,\rho\, O\,. \tag{4.2}$$

La probabilidad de encontrar al sistema en un estado particular $|i\rangle$, (que supondremos normalizado) es entonces

$$p_i = \langle P_i \rangle = \mathrm{Tr}\,\rho\, P_i = \langle i|\rho|i\rangle\,, \tag{4.3}$$

donde $P_i = |i\rangle\langle i|$ es el proyector ortogonal sobre el estado $|i\rangle$.

En el caso de un sistema cuántico en un estado puro $|i\rangle$, ρ es entonces el proyector ortogonal sobre el espacio generado por $|i\rangle$:

$$\rho = |i\rangle\langle i|\,, \tag{4.4}$$

y satisface $\rho^2 = \rho$. En el caso general, la descomposición espectral de ρ la escribiremos como

$$\rho = \sum_i p_i |i\rangle\langle i|\,, \tag{4.5}$$

donde $\{p_i, i = 1, \ldots, n\}$ son los autovalores de ρ ($p_i \geq 0$, $\sum_i p_i = 1$) y $\{|i\rangle, i = 1, \ldots, n\}$ los correspondientes autovectores normalizados ($\langle i|i'\rangle = \delta_{ii'}$). El caso puro corresponde a $p_i = 1$ para un cierto estado y 0 para todos los demás. En el caso general,

tenemos $\rho^2 \leq \rho$ (es decir, $\rho^2 - \rho$ es un operador con autovalores $-p_i(1-p_i)$ negativos o nulos).

La entropía de von Neumann[11, 18, 19] se define como

$$S(\rho) = -\mathrm{Tr}\,\rho\log\rho \tag{4.6}$$
$$= -\sum_i p_i \log p_i\,, \tag{4.7}$$

y es una medida de la falta de información asociada al estado ρ. Tenemos $S(\rho) \geq 0$, con $S(\rho) = 0$ únicamente si ρ es un estado puro ($\rho^2 = \rho$). $S(\rho)$ será por el contrario máxima ($S(\rho) = \log n$ si el espacio de Hilbert del sistema tiene dimensión n) si el estado ρ es máximamente "mezclado" $\rho_n = I_n/n$, donde I_n denota el operador identidad, tal que $p_i = 1/n\;\forall\, i$.

4.2. Sistemas Compuestos y Estados Reducidos

Dados dos sistemas cuánticos distinguibles, que denotaremos como A y B, con sendos espacios de Hilbert $\mathcal{H}_A$ y $\mathcal{H}_B$ y espacio de Hilbert conjunto $\mathcal{H}_A \otimes \mathcal{H}_B$, el estado conjunto estará determinado por una cierta *matriz densidad conjunta* ρ_{AB}. La entropía conjunta es por lo tanto

$$S(A,B) = S(\rho_{AB}) = -\mathrm{Tr}\,\rho_{AB}\log\rho_{AB}\,. \tag{4.8}$$

Un observable *local* en el sistema A es un observable de la forma $O_A \equiv O_A \otimes I_B$, donde I_B denota la identidad en $\mathcal{H}_B$. Su valor medio es entonces

$$\langle O_A\rangle = \mathrm{Tr}\,\rho_{AB}O_A = \mathrm{Tr}_A\,\rho_A O_A\,, \tag{4.9}$$

donde hemos definido la *matriz densidad reducida* [11, 18]

$$\rho_A = \mathrm{Tr}_B\,\rho_{AB} \tag{4.10}$$

la cual determina completamente los valores medios de todo observable local en A. Explícitamente, $\langle i|\rho_A|j\rangle = \sum_k \langle ik|\rho_{AB}|jk\rangle$, donde $|ik\rangle \equiv |i\rangle \otimes |k\rangle$ son los estados de una base producto ortonormal de $\mathcal{H}_A \otimes \mathcal{H}_B$. Análogamente,

$$\rho_B = \mathrm{Tr}_A\,\rho_{AB}\,,$$

determina los valores medios de cualquier operador local O_B en B. Las entropías locales son

$$S(A) = -\mathrm{Tr}\,\rho_A\log\rho_A\,,\quad S(B) = -\mathrm{Tr}\,\rho_B\log\rho_B\,.$$

El estado conjunto es no correlacionado si y solo si $\rho_{AB} = \rho_A \otimes \rho_B$, es decir, si y solo si es un estado producto, en cuyo caso sus autovalores son $p_{ij} = p_i^A p_j^B$ con p_i^A y p_j^B los

autovalores de ρ_A y ρ_B respectivamente. En tal caso las entropías satisfacen $S(A,B) = S(A) + S(B)$, como es fácil ver de la definición (4.8).

4.3. Información Mutua y Entropía Condicional

Podemos ahora definir la **información mutua** como

$$I(A:B) \;=\; S(\rho_A) + S(\rho_B) - S(\rho_{AB})\,. \tag{4.11}$$

Esta cantidad es una medida de la correlación (total) entre A y B [11, 18]. Si $\rho_{AB} = \rho_A \otimes \rho_B$, $S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$ y por lo tanto $I(A:B) = 0$. En caso contrario $I(A:B) > 0$.

Esta positividad de $I(A:B)$ es conceptualmente evidente: $S(A) + S(B)$ es una medida de la falta de información cuando sólo se dispone de información sobre los valores medios de todos los observables locales (es decir, cuando se conoce sólo ρ_A y ρ_B), mientras que $S(A,B)$ mide la falta de información cuando se conoce además toda la información sobre las correlaciones, es decir, sobre todos los valores medios de observables generales del tipo $O_{AB} = O_A \otimes O_B$. Por lo tanto $S(A,B) \leq S(A) + S(B)$.

Clásicamente, es decir, para sistemas descriptos por densidades de probabilidad, se tiene además

$$S(A,B) \geq S(A), \quad S(A,B) \geq S(B) \tag{4.12}$$

Las entropías condicionales $S(A|B)$ y $S(B|A)$ pueden definirse como

$$S(A|B) = S(A,B) - S(B), \quad S(B|A) = S(A,B) - S(A) \tag{4.13}$$

y son por lo tanto cantidades no negativas en sistemas clásicos.

Sin embargo, la desigualdad (4.12) no sigue siendo válida en sistemas cuánticos, es decir, en sistemas descriptos por operadores densidad. En otras palabras, en sistemas cuánticos la entropía global puede ser menor que las entropías locales, y las entropías condicionales definidas como en (4.13) pueden por lo tanto ser negativas.

A modo de ejemplo, consideremos un par de qubits o espines $1/2$ en un estado de Bell, por ejemplo

$$|\Psi\rangle = \frac{|\uparrow\uparrow\rangle + |\downarrow\downarrow\rangle}{\sqrt{2}}\,, \tag{4.14}$$

donde $|\uparrow\uparrow\rangle = |\uparrow\rangle \otimes |\uparrow\rangle$ denota un estado con ambos espines en la dirección z positiva. El estado $\rho = |\Psi\rangle\langle\Psi|$ es un estado puro y por lo tanto,

$$S(\rho_{AB}) = 0\,.$$

No obstante, los estados reducidos son máximamente mezclados:

$$\rho_A = \rho_B = \frac{1}{2} I_2 = \frac{1}{2}(|\uparrow\rangle\langle\uparrow| + |\downarrow\rangle\langle\downarrow|)\,.$$

Por lo tanto,

$$S(\rho_A) = S(\rho_B) = 1\,, \tag{4.15}$$

tomando el logaritmo en base 2. Esto implica $S(A) = S(B) > S(A,B) = 0$, a diferencia de cualquier sistema clásico. Más aun, los estados locales están máximamente mezclados (es decir, máximamente "desordenados") a pesar de que el estado global es puro (es decir, máximamente "ordenado"). Para este estado tenemos entonces

$$I(A:B) = 2$$

$$S(A|B) = S(B|A) = -1\,.$$

Como veremos a continuación, la violación de las desigualdades clásicas (4.12) puede darse solo cuando el estado ρ es entrelazado.

4.4. Entrelazamiento de Estados Puros

Si un estado cuántico puro $|\Psi_{AB}\rangle$ de un sistema conjunto $A+B$ se puede escribir como estado producto, no posee entrelazamiento y se lo denomina *separable*. Por otro lado un estado *entrelazado* no puede descomponerse en un producto de estados:

$$|\Psi_{AB}\rangle = |\Psi_A\rangle|\Psi_B\rangle \quad \Rightarrow \quad |\Psi_{AB}\rangle \; separable \tag{4.16}$$

$$|\Psi_{AB}\rangle \neq |\Psi_A\rangle|\Psi_B\rangle \quad \Rightarrow \quad |\Psi_{AB}\rangle \; entrelazado \tag{4.17}$$

Las entropías de los subsistemas de un estado puro son idénticas (véase (4.22) y permiten definir la *entropía de entrelazamiento* [11, 16], que cuantifica el **entrelazamiento** de un estado cuántico puro bipartito, como

$$E(A,B) = S(A) = S(B)\,. \tag{4.18}$$

$E(A,B)$ es una medida de las correlaciones cuánticas en el estado. Si $|\Psi_{AB}\rangle$ es separable, entonces $\rho_A = |\Psi_A\rangle\langle\Psi_A|$, $\rho_B = |\Psi_B\rangle\langle\Psi_B|$ y $E(A,B) = 0$.

En el caso puro $E(A,B)$ es menos la entropía condicional:

$$S(A|B) = S(B|A) = -E(A,B)\,, \tag{4.19}$$

pues $S(A,B)=0$. Mientras que la correspondiente información mutua es

$$I(A:B)=S(A)-S(A|B)=2S(A)=2E(A,B)\,. \tag{4.20}$$

Podemos considerar a $I(A:B)$ como una medida de todas las correlaciones en el sistema, mientras que a $E(A,B)$ como una medida de correlaciones puramente cuánticas.

Una forma de determinar si un estado cuántico es entrelazado es a través de la *descomposición de Schmidt* del estado [11]: Existen siempre bases locales $\{|k_A\rangle\}$ y $\{|k_B\rangle\}$ ortonormales, en las que $|\Psi\rangle$ puede escribirse en la forma

$$|\Psi\rangle=\sum_{k=1}^{n_s}\sigma_k|k_A\rangle|k_B\rangle\,, \tag{4.21}$$

donde n_s es el número de Schmidt y $\sigma_k>0$, $\sum_{k=1}^{n_s}\sigma_k^2=1$. Las matrices densidad reducidas están entonces dadas por

$$\rho_A=\sum_k\sigma_k^2|k_A\rangle\langle k_A|\,,\quad \rho_B=\sum_k\sigma_k^2|k_B\rangle\langle k_B|\,. \tag{4.22}$$

Estas son isospectrales por lo que $S(A)=S(B)$. El caso separable corresponde a $n_s=1$, donde $E(A,B)=0$, mientras que el caso entrelazado a $n_s\geq 2$, en el que

$$E(A,B)=-\sum_{k=1}^{n_s}\sigma_k^2\log\left(\sigma_k^2\right) \tag{4.23}$$

La descomposición de Schmidt puede obtenerse a partir de la *descomposición en valores singulares* de la matriz de los coeficientes de expansión de $|\Psi\rangle$ en una base producto ortogonal, arbitraria [11], siendo los σ_k los valores singulares de dicha matriz. En el caso del estado de Bell (ecuación 4.14), ya está expresado en una base de Schmidt, con $n_s=2$ y $\sigma_1=\sigma_2=1/\sqrt{2}$.

El entrelazamiento es considerado un *recurso esencial* en información cuántica [11, 15], ya que permite formas radicalmente nuevas de intercambio y procesamiento de la información, tales como la teleportación cuántica [20] y la computación cuántica [11].

4.5. Entrelazamiento de Estados no Puros

La definición de entrelazamiento cuántico es más compleja para estados ρ generales no necesariamente puros ($\rho^2\leq\rho$). De hecho, en el caso general no es posible obtener un método general para determinar si el estado es entrelazado, en un número finito de pasos. Por lo tanto tampoco es posible obtener una medida computable del mismo.

Según la definición introducida por R.F. Werner en 1989 [21], un estado cuántico general es *entrelazado* si no es *separable* o *clásicamente correlacionado*, en cuyo caso puede

ser escrito como una combinación convexa de estados producto, es decir, una superposición estadística de estados no correlacionados:

$$\rho = \sum_\alpha q_\alpha \rho_A^\alpha \otimes \rho_B^\alpha, \quad q_\alpha \geq 0, \quad \Rightarrow \quad \rho \; separable \tag{4.24}$$

$$\rho \neq \sum_\alpha q_\alpha \rho_A^\alpha \otimes \rho_B^\alpha, \quad q_\alpha \geq 0, \quad \Rightarrow \quad \rho \; entrelazado \tag{4.25}$$

donde $\sum_\alpha q_\alpha = 1$. En particular, un estado producto $\rho_{AB} = \rho_A \otimes \rho_B$, es decir, un estado no correlacionado, es un estado separable. Pero también lo es cualquier combinación convexa de los mismos. El argumento [21] es que los estados separables pueden ser generados mediante operaciones locales y comunicación clásica (es decir, por (*LOCC: Local Operations and Classical Communication*) [11]) y por lo tanto no contienen correlaciones cuánticas. ‘ En otras palabras, dos personas a cierta distancia pueden, a través de comunicación clásica, acordar preparar un estado producto $|\Psi_A\rangle|\Psi_B\rangle$, pero también una combinación estadística de estados producto: A tira un dado y de acuerdo al valor de este prepara $|\Psi_A^\alpha\rangle$, $\alpha = 1, \ldots, 6$ y avisa a B, quien prepara el correspondiente estado $|\Psi_B^\alpha\rangle$, originando así una combinación convexa del tipo (4.24) ($\rho = \sum_{\alpha=1}^6 \frac{1}{6} |\Psi_A^\alpha\rangle\langle\Psi_A^\alpha| \otimes |\Psi_B^\alpha\rangle\langle\Psi_B^\alpha|$).

Por otro lado un estado entrelazado no puede ser escrito de la forma anterior con coeficientes q_α positivos. Estos se generan únicamente por medio de una interacción cuántica entre los sistemas. Pueden generarse como autoestados de un Hamiltoniano que contenga términos de interacción $\sum_\alpha o_A^\alpha \otimes o_B^\alpha$, o haciendo evolucionar un estado inicialmente separable con un Hamiltoniano del tipo anterior [11, 22] (de forma que el operador evolución $U(t) = \exp[-iHt/\hbar]$ no sea un producto de operadores de evolución locales $U_A(t) \otimes U_B(t)$).

Los estados ρ diagonales en una base producto: $\rho = \sum_{i,j} p_{ij} |ij\rangle\langle ij|$ son un caso particular de estado separable. En el caso general, los distintos términos en (4.24) no son necesariamente conmutantes.

En el caso puro, la definición (4.24) coincide por supuesto con la previa dada en la ecuación (4.17): Si $\rho_{AB}^2 = \rho_{AB}$, la combinación convexa (4.24) es necesariamente un estado producto $\rho_A \otimes \rho_B$, con ρ_A y ρ_B puros.

4.6. Criterios Básicos de Separabilidad

En general, excepto en casos simples como el de dos qubits, no es fácil determinar si un estado no puro, es separable o entrelazado. En realidad es un problema considerado en general “ *hard* ” [23].

El **criterio de la traspuesta parcial**, introducido por Asher Peres en 1996 [24], proporciona un criterio de separabilidad simple, computable y necesario, pero en general no suficiente. Es decir,

$$\rho_{AB} \; separable \; \Rightarrow \rho_{AB}^{t_A} \geq 0 \,, \tag{4.26}$$

donde t^A denota *trasposición parcial* [11] ($\langle ij|\rho_{AB}^{t_A}|kl\rangle = \langle kj|\rho_{AB}|il\rangle$). Es decir, si $\rho_{AB}^{t_A}$ tiene algún autovalor negativo entonces ρ_{AB} es entrelazado. Pero si todos sus autovalores son no-negativos puede ser aún entrelazado. Sólo en el caso de dos qubits o qubit/qutrit, el presente criterio es *necesario y suficiente* [24, 25].

Interpretémoslo de otra forma: Si tenemos $|ij\rangle\langle kl| = |i\rangle\langle k| \otimes |j\rangle\langle l|$ entonces

$$(|ij\rangle\langle kl|)^{T_B} = |il\rangle\langle kj| = |i\rangle\langle k| \otimes |l\rangle\langle j|$$

Si ρ_{AB} es separable entonces

$$\rho_{AB}^{T_B} = \sum_\alpha p_\alpha (\rho_A^\alpha \otimes \rho_B^\alpha)^{T_B} = \sum_\alpha p_\alpha \rho_A^\alpha \otimes (\rho_B^\alpha)^T$$

La traspuesta de ρ_B^α no cambia los autovalores, entonces la traza sigue siendo 1. $(\rho_B^\alpha)^T = \rho_B^\alpha$, $\left((\rho_B^\alpha)^T\right)^T = (\rho_B^\alpha)^T$, $Tr(\rho_B^\alpha)^T = Tr\rho_B^\alpha$

Ej:

$$|\psi_{AB}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$\rho_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}| = \frac{1}{2}\left(\underbrace{\overset{|0\rangle\langle 0|\otimes|0\rangle\langle 0|}{|00\rangle\langle 00|} + \overset{|1\rangle\langle 1|\otimes|1\rangle\langle 1|}{|11\rangle\langle 11|}}_{\text{esto es separable}} + |00\rangle\langle 11| + |11\rangle\langle 00|\right)$$

$$\rho_{AB}^{T_B} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11| + |01\rangle\langle 10| + |10\rangle\langle 01|)$$

$$\rho_{AB}^{T_B} = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

vemos arriba como era ρ_{AB} sin transponer y vemos como afecta. Los autovalores son

$$\lambda\left(\rho_{AB}^{T_B}\right) = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right)$$

cuando aplicamos la traza parcial a un estado entrelazado obtenemos un autovalor negativo, entonces aplicar la traza parcial me genera un $\rho_{AB}^{T_B}$ no es un operador densidad.

Resumen: el criterio me dice que si ρ_{AB} es separable entonces $\rho_{AB}^{T_B} \geq 0$ entonces $\lambda\left(\rho_{AB}^{T_B}\right) \geq 0$ (es decir sigue siendo un operador densidad). El contrarecíproco sería que $\rho_{AB}^{T_B} \not\geq 0$ es decir $\exists \lambda_i\left(\rho_{AB}^{T_B}\right) < 0$, entonces ρ_{AB} es entrelazado.

El **criterio entrópico estándar** se basa en que los estados separables al igual que los sistemas clásicos, son siempre más desordenados globalmente que localmente [25]:

$$\rho \text{ separable } \Rightarrow S(A,B) \geq S(A)\,, \tag{4.27}$$

y análogamente, $S(A,B) \geq S(B)$. Corresponden pues a entropías condicionales $S(A|B)$ y $S(B|A)$ *positivas*.

Los estados entrelazados pueden satisfacer, como vimos, $S(A,B) < S(A)$, pero a diferencia del caso puro, en el caso no puro esta condición no es necesaria: Existen también estados entrelazados que son más desordenados globalmente que localmente ($S(A,B) > S(A)$, $S(A,B) > S(B)$). Notemos también que en el caso no puro, $S(A)$ no es necesariamente igual a $S(B)$.

El presente criterio entrópico (ρ_{AB} separable $\Rightarrow S(A,B) \geq S(A)$) puede generalizarse en realidad a otras entropías (por ejemplo, del tipo $S(\rho) = \mathrm{Tr} f(\rho)$, con f cóncava y $f(0) = f(1) = 0$ [26]), dando lugar al **criterio entrópico generalizado** [27], que es más fuerte que el criterio entrópico basado en la entropía de von Neumann [25] y equivalente al criterio general de desorden [28].

4.7. Medidas de Entrelazamiento

La medida de entrelazamiento en estados no puros es un tema que no está cerrado y es aún más difícil. Usualmente se utiliza como medida el entrelazamiento de formación, definido por la denominada "*Convex Roof Extension*" de la definición para estados puros [15, 17]:

$$E(A,B) \equiv E(\rho_{AB}) = \underset{\sum_i q_i |\Psi_i\rangle\langle\Psi_i| = \rho_{AB}}{\mathrm{Min}} \sum_i q_i\, E(|\Psi_i\rangle\langle\Psi_i|) \tag{4.28}$$

es decir, es el mínimo, entre todas las representaciones posibles de ρ_{AB} como combinación convexa de estados puros $|\Psi_i\rangle$ (no necesariamente ortogonales), del promedio del entrelazamiento en los mismos, definido de acuerdo a (4.18). En general, la cantidad (4.28) no es computable de forma exacta.

4.7.1. Concurrencia

La gran excepción es el caso de dos qubits (o sea, dos sistemas con espacio de Hilbert local de dimensión 2, tal como un par de espines $1/2$), donde W.K. Wootters logró obtener una fórmula general computable en 1998 por medio de la llamada concurrencia C_{AB} [29]:

$$E(A,B) \;\; = \;\; -\sum_{\nu=\pm} q_\nu \log q_\nu, \tag{4.29}$$

donde

$$q_\nu = \frac{1\pm\sqrt{1-C^2(A,B)}}{2}\,, \tag{4.30}$$

$$C(A,B) = \mathrm{Max}[2\lambda_M - \mathrm{Tr}R, 0]\,. \tag{4.31}$$

Aquí λ_M es el autovalor máximo de la matriz $R = \sqrt{\rho_{AB}^{1/2}\tilde{\rho}_{AB}\rho_{AB}^{1/2}}$, con $\tilde{\rho}_{AB} = \sigma_y \otimes \sigma_y \rho_{AB}^* \sigma_y \otimes \sigma_y$ en la base estándar, compuesta por los autoestados producto de $\sigma_z \otimes \sigma_z$. Aquí $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ denota las matrices de Pauli.

Se verifica

$$0 \leq C(A,B) \leq 1\,, \quad 0 \leq E(A,B) \leq 1 \tag{4.32}$$

con $E(A,B) = C(A,B) = 1$ para un estado de Bell (que es, por lo tanto, un estado máximamente entrelazado), y $E(A,B) = C(A,B) = 0$ para un estado separable, siendo $E(A,B)$ una función estrictamente creciente de $C(A,B)$.

Para el caso de un estado puro arbitrario de dos qubits, se ve que (4.29) se reduce a la entropía $S(A) = S(B)$ de cualquiera de los qubits, dada por la expresión (4.23) con $n_s = 2$. En tal caso $C(A,B) = 2\sqrt{\sigma_1\sigma_2}$.

4.7.2. Negatividad

La negatividad es un estimador de entrelazamiento computable para estados mixtos de cualquier dimensión [30-32], definida por

$$N_{AB} = (\mathrm{Tr}\,|\rho_{AB}^{\mathrm{t_A}}| - 1)/2\,, \tag{4.33}$$

donde $\rho_{AB}^{\mathrm{t_2}}$ denota la traspuesta parcial de ρ_{AB}. La Ec. (4.33) es simplemente el valor absoluto de la suma de los autovalores negativos de $\rho_{AB}^{\mathrm{t_A}}$. Si ρ_{AB} es un estado puro ($\rho_{AB} = |\psi_0\rangle\langle\psi_0|$), la Ec. (4.33) se reduce a una entropía de entrelazamiento generalizada,

$$N_{AB} = [(\mathrm{Tr}\,\sqrt{\rho_A})^2 - 1]/2 = \sum_{i<j} \lambda_i^1 \lambda_j^1 \tag{4.34}$$

donde $\rho_A = \mathrm{Tr}_B\,|\psi_0\rangle\langle\psi_0|$ es el estado reducido de A y λ_i^1 sus autovalores. En este caso el estado es entrelazado si y solo si $N_{AB} > 0$. Consecuentemente, la Ec. (4.34) se anula para ρ_A puro ($|\psi_0\rangle$ separable), y alcanza su máximo para ρ_A máximamente mezclado (es decir, $|\psi_0\rangle$ máximamente entrelazado), en cuyo caso $N_{AB} = (d-1)/2$, con $d = \mathrm{Min}[d_A, d_B]$ (en particular, $N_{AB} = s$ para un par de espines s).

En el caso mixto general, $N_{AB} > 0$ implica entrelazamiento de ρ_{AB}, pero $N_{AB} = 0$ no implica necesariamente separabilidad, salvo para sistemas qubit-qubit o qubit-qutrit [25], ya que existen ciertos estados mixtos entrelazados (*bound entangled states*) que igualmente cumplen $N_{AB} = 0$. No obstante, dada su computabilidad, N_{AB} es corrientemente utilizada como una medida o estimador de entrelazamiento de estados mixtos.

Ejemplo: Sistema de 2 qubits

$$\rho_{AB} = p|\psi_{AB}\rangle\langle\psi_{AB}| + (1-p)\frac{I_{AB}}{4}$$

$\frac{I_{AB}}{4}$ este es el estado máximamente mezclado.

¿Cuál es el valor umbral de p para que exista entrelazamiento?

$$\rho_{AB} = \begin{pmatrix} \frac{p}{2}+\frac{1-p}{4} & 0 & 0 & \frac{p}{2} \\ 0 & \frac{1-p}{4} & 0 & 0 \\ 0 & 0 & \frac{1-p}{4} & 0 \\ \frac{p}{2} & 0 & 0 & \frac{1-p}{4} \end{pmatrix}$$

Si hacemos la transpuesta parcial,

$$\rho_{AB}^{T_B} = \begin{pmatrix} \frac{p}{2}+\frac{1-p}{4} & 0 & 0 & 0 \\ 0 & \frac{1-p}{4} & \frac{p}{2} & 0 \\ 0 & \frac{p}{2} & \frac{1-p}{4} & 0 \\ 0 & 0 & 0 & \frac{1-p}{4} \end{pmatrix}$$

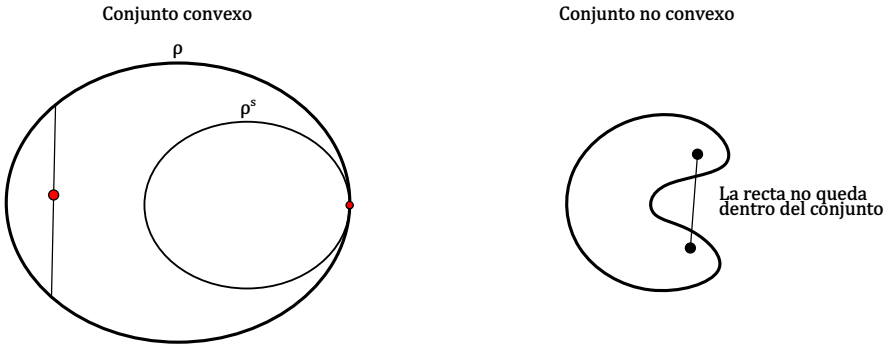
$$\lambda\left(\rho_{AB}^{T_B}\right) = \left(\frac{p}{2}+\frac{1-p}{4}, \frac{p}{2}+\frac{1-p}{4}, \frac{p}{2} \pm \frac{1-p}{4}\right)$$

$$\frac{1-p}{4} - \frac{p}{2} < 0 \rightarrow 1-3p < 0 \rightarrow p > \frac{1}{3}$$

4.7.3. Testigo de entrelazamiento

Un testigo de entrelazamiento es un operador autoadjunto O_{AB} tal que $Tr\rho_{AB\,sep}O_{AB} \geq 0\ \forall\rho_{AB\,sep}$. Pero, dado un cierto ρ_{AB}^{E} entrelazado $Tr\rho_{AB}^{E}O_{AB} < 0$ (esto vale solo para un cierto ρ_{AB}^{E} no para todos).

Dado ρ_{AB} entrelazado $\exists\ O_{AB}$ tal que $Tr\rho_{AB}O_{AB} < 0$, pero la traza de cualquier operador separable $Tr\rho_{AB}^{S}O_{AB} \geq 0\ \forall\rho_{AB}^{S}$. **Demostración**



1) El conjunto de todos los ρ de un sistema físico es un conjunto convexo. Quiere decir que si ρ_1 es operador densidad y ρ_2 es operador densidad entonces $p\rho_1 + (1-p)\rho_2$ es un operador densidad $\forall p \in [0,1]$.

Entonces si supongamos que este es el conjunto de los operadores densidad y el borde de los ρ son los estados puros. Todo conjunto convexo se pueden generar a partir de unos estados borde, estados límite. Porque del punto de vista matemático un punto que está en el medio entre dos estados de borde lo puedo escribir como combinación lineal de dos estados de borde de la forma $p\rho_1 + (1-p)\rho_2$.

Dentro del conjunto convexo de todos los operadores densidad de un sistema dado. En el borde estados puros. Adentro está el conjunto de los ρ separables.

2) El conjunto de los operadores densidad separables para un dado sistema físico es convexo. La robustes de un operador separable que mezclas cosas y seguis estando ahí adentro no la tienen los operadores producto, una mezcla de producto no es un operador producto. Por eso el concepto de separabilidad es importante.

$$\begin{matrix}\rho_1 = \sum_\alpha p_\alpha^1 \rho_A^{1\alpha} \otimes \rho_B^{1\alpha} \\ \rho_2 = \sum_\alpha p_\alpha^2 \rho_A^{2\alpha} \otimes \rho_B^{2\alpha}\end{matrix} \Rightarrow q\rho_1 + (1-q)\rho_2 = \sum_\alpha q p_\alpha^1 \rho_A^{1\alpha} \otimes \rho_B^{1\alpha} + (1-q) p_\alpha^2 \rho_A^{2\alpha} \otimes \rho_B^{2\alpha}$$

Esto sigue siendo un operador densidad separable, mientras $q \in [0,1]$.

Desde el punto de vista físico la propiedad de convexidad es importante porque te esta diciendo que si yo genero algo en este conjunto y hago mezclas de eso, es decir que por ej. si tiro un dado cuando en el dado sale 1 genero un cierto estado separable, cuando me sale 2 otro, y así, y el estado promedio que sale es un estado separable también. Es decir mezclando esas cosas no me voy del conjunto.

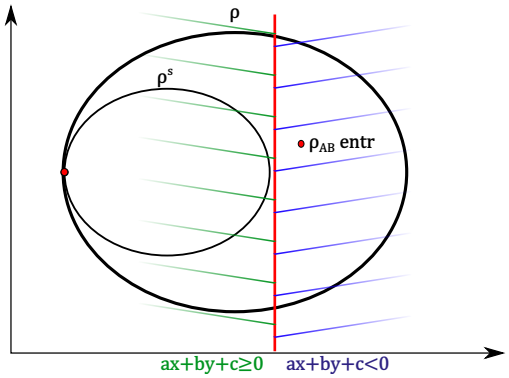
El conjunto de estados producto no es convexo, porque no son conmutantes. Los estados separables tienen en general autoestados entrelazados, ie el hecho que sea una combinación convexa de productos como estos estados ($\rho_{AB} = \sum_\alpha p_\alpha \rho_A^\alpha \otimes \rho_B^\alpha$) que estamos sumando, donde cada α es un índice de estado ρ_A, ρ_B cualquiera donde no tienen porque ser conmutantes, son suma de productos no conmutantes. Al sumar todo esto al ser

no conmutantes, si uno analiza esto, no todos o una buena parte son entrelazados. Pero aún así el estado separable es generable por operaciones locales y conmunicación clásica LOCC.

Notar que el conjunto de los operadores densidad ρ se toca en sólo punto con el de los ρ_s, es un punto donde es separable y puro al mismo tiempo y es uno sólo porque **implica** que ρ es un producto

$$\rho = |k_A\rangle|k_A\rangle \otimes \langle k_B|\langle k_B| \rightarrow \rho = |\psi_{AB}\rangle\langle\psi_{AB}|$$

Volvamos a la **demostración**, supongamos que tenemos un ρ_{AB} entrelazado, y tenemos la recta roja que me divide el espacio en 2 semiplanos (sup que estamos en 2 d)



Esto pasa a $Tr\rho_{AB}O_{AB} \geq 0$ y a $Tr\rho_{AB}O_{AB} \geq 0$, siendo los coeficientes $a,\ b,\ c$ sería el operador testigo O_{AB} y las coordenadas $x,\ y$ son los elementos del operador ρ_{AB} en una base de operadores y esta condición sobre $Tr\rho_{AB}O_{AB}$ es una proyección lineal de ρ_{AB} sobre alguna base. El hecho que ρ^s sea convexo hace que exista una recta entre ρ entrelazado y ρ^s, entonces se prende la «lámparita» cuando estoy de uno de los lados.■

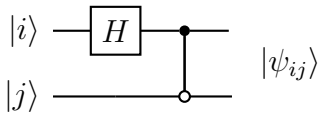
Podemos ver que el entrelazamiento es muy débil porque ponele que genero un estado que este del lado izquierdo que caiga fuera del conjunto de los separables, eso no es un conjunto convexo entonces me va a fallar. Es decir, en cuanto tenga probabilidad de generar un entrelazado ahí se cae el entrelazamiento, y eso puede pasar si hay ruido. En cambio con los separables no pasa eso.

El conjunto de estados entrelazados no es convexo.

Ejemplo

Supongamos que tenemos los estados de Bell

$$\left\{ \begin{array}{l} \left|\psi^{00}_{01}\right\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}} \\ \left|\psi^{10}_{11}\right\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}} \end{array} \right\} \text{base de estados de 2 qubits de } \mathbb{C}^2 \otimes \mathbb{C}^2$$



Tenemos que el estado $|\psi_{ij}\rangle\langle\psi_{ij}|$ es entrelazado pero

$$\sum_{i,j=0}^{1} |\psi_{ij}\rangle\langle\psi_{ij}|\frac{1}{4} = \frac{I_{AB}}{4} \text{ es el estado máximamente mezclado}$$

Como la identidad es la identidad en todas las bases, entonces lo anterior es igual a

$$= \frac{1}{4}\sum_{i,j=0}^{1} |i\rangle|j\rangle\langle i|\langle j| = \frac{1}{4}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$$

genero un ruido al azar. Esto implica que las medidas de entrelazamiento no son cóncavas sino son convexas ie el entrelazamiento de una mezcla tiene que ser menor que la mezcla de entrelazamientos. El entrelazamiento de un promedio siempre es menor o igual que el promedio de los entrelazamientos.

4.8. Fidelidad

La fidelidad [11] es una medida de la distancia entre dos estados cuánticos (puros o no puros). Se define como

$$F(\rho, \rho') = \mathrm{Tr}\sqrt{\rho^{1/2}\rho'\rho^{1/2}}\,. \tag{4.35}$$

Para estados puros $\rho = |\psi\rangle\langle\psi|$, $\rho' = |\psi'\rangle\langle\psi'|$, $F(\rho, \rho')$ se reduce al modulo del *overlap*:

$$F(\rho, \rho') = |\langle\psi|\psi'\rangle|\,. \tag{4.36}$$

En ambos casos, la fidelidad es un número entre 0 y 1,

$$0 \leq F \leq 1\,,$$

con $F(\rho, \rho') = 1$ si y solo si $\rho = \rho'$ y $F(\rho, \rho') = 0$ si y solo si ρ y ρ' tienen soportes ortogonales.

La fidelidad está relacionada con otra cantidad que mide cuan diferentes son dos estados, conocida como medida o métrica de Wootters. Esta última puede evaluarse en función de la primera por la relación

$$B(\rho, \rho') = \arccos F(\rho, \rho') \tag{4.37}$$

Esta medida define una distancia entre los operadores estadísticos, ya que es una cantidad semidefinida positiva y simétrica que satisface la desigualdad triangular ($B(\rho, \rho') \leq B(\rho, \rho'') + B(\rho'', \rho')$).

4.8.1. Entrelazamiento de formación

Miremos primero como calculo el valor medio de la energía

$$\langle H \rangle = Tr\rho H$$

con H un hamiltoniano, con $\rho = \sum_i p_i |i\rangle\langle i|$, luego $\langle H \rangle = \langle i|H|i\rangle = \sum_i \langle i|H|i\rangle p_i$ implica un valor medio cuántico con distribución de probabilidad y un valor medio clásico con p_i.

Nosotros sabemos que el entrelazamiento de un estado puro $E(|\psi_{AB}\rangle) = S(\rho_A) = S(\rho_B)$, con $\rho_A = Tr_B|\psi_{AB}\rangle\langle\psi_{AB}|$, entonces uno podría definir (haciendo un razonamiento para comenzar, luego veremos que en realidad es incorrecto) $E(\rho_{AB}) = \sum_i p_i E(|\psi_{AB}\rangle)$, esta definición no tiene sentido por el ejemplo que vimos recién de estados de Bell 4.7.3, si aplico esta definición de entrelazamiento a la expresión a una mezcla de estados de Bell me da 1 y si lo aplico a una mezcla de estados producto me da 0, es decir me queda $0 = 1$. Tiene que ser una propiedad del vector pero no debe depender de la representación que elija al vector.

Definimos al *entrelazamiento de formación* como

$$E(\rho_{AB}) = \underset{\left\{p_i \left|\psi^i_{AB}\right\rangle / \sum_i p_i |\psi^i_{AB}\rangle\langle\psi^i_{AB}| = \rho_{AB}\right\}}{\text{Min}} \sum_i p_i E\left(\left|\psi^i_{AB}\right\rangle\right)$$

Tomo el mínimo sobre todas las representaciones. Esto es consistente ya que cumple que $E(\rho_{AB}) \geq 0$, $E(\rho_{AB}) = 0 \iff \rho_{AB}$ separable.

Este no es un criterio necesario y suficiente porque está muy bien pero no es computable (no es física, porque tenés que pensar sobre todas las posibles mezclas que te da un estado, es un espacio infinito).

Caso de 2 qubits. Wootters

Logró evaluar de forma analítica $E(\rho_{AB})\ \forall \rho_{AB}$ de 2 qubits.

4.8.2. Fórmula de Wootters (2 qubits)

$$E(\rho_{AB}) = -\sum_{i=0,1} p_i \log p_i = S(\rho_A) = S(\rho_B)$$

Donde $p_{\substack{0\\1}} = \frac{1 \pm \sqrt{1-c^2}}{2}$, con c la concurrencia. Siendo $c = 2\lambda_{max}(R) - Tr(R)$ y $R = \sqrt{\rho^{1/2}_{AB} \tilde{\rho}_{AB} \rho^{1/2}_{AB}}$, con $\tilde{\rho}_{AB} = \sigma_y \otimes \sigma_y \rho^*_{AB} \sigma_y \otimes \sigma_y$.

Para **estados puros** $E(\rho_{AB}) = S(\rho_A) = S(\rho_B)$. Para estados mezcla $S(\rho_A) \neq S(\rho_B)$ y no mide ni entrelazamiento ni correlación.

Para estados puros la concurrencia la podemos calcular como $c(\rho_{AB}) = \sqrt{1 - Tr(\rho_{AB}^2)}$, es decir todas las medidas de correlación o entrelazamiento bien definidas cuando son medidas para un estado puro deben reducirse a una medida de entropía de estado local (no necesariamente la de Shannon). La $Tr(\rho_{AB}^2)$ se llama pureza, ya que da 1 para estados puros ya que $\rho_{AB}^2 = \rho_{AB}$.

Bibliografía

1. (a) T. Ramos, H. Pichler, A. Daley y P. Zoller. *Phys. Rev. Lett.* 113, 2014, pág. 237203; (b) A. Glaetzle, M. Damonte, R. Nath, C. Gross, I. Bloch y P. Zoller. *Phys. Rev. Lett.* 114, 2015, pág. 173002; (c) I. Bloch, J. Dalibard y W. Zwerger. *Rev. Mod. Phys.* 80, 2006, pág. 885.
2. (a) J. Perk, H. Capel, M. Zuilhof y T. Siskens. *Phys. A* 81, 1975, pág. 319; (b) T. Siskens, H. Capel y J. Perk. *Phys. Lett. A* 53, 1975, pág. 21.
3. (a) J. Perk, H. Capel y T. Siskens. *Phys. A* 89, 1977, pág. 304; (b) J. Perk y H. Capel. *Phys. A* 92, 1978, pág. 163; (c) J. Perk y H. Au-Yang. *J. Stat. Phys.* 135, 2009, pág. 599; (d) J. Perk y H. Capel. *Phys. A* 92, 1978, pág. 163; (e) J. Perk y H. Au-Yang. *J. Stat. Phys.* 135, 2009, pág. 599.
4. (a) E. Kutznetsova y E. Fel'dman. *JETP. Lett.* 102, 2006, pág. 882; (b) E. Fel'dman y M. Rudavets. *JETP. Lett.* 81, 2005, pág. 47; (c) S. Doronin, A. Pyrkov y E. Fel'dman. *JETP. Lett.* 85, 2007, pág. 519.
5. (a) C. Majundar y D. Gosh. *J. Math. Phys.* 10, 1969, pág. 1388; (b) C. Majundar y D. Gosh. *J. Math. Phys.* 10, 1969, pág. 1399; (c) B. Shastry y B. Sutherland. *Phys. Rev. Lett.* 47, 1981, pág. 964.
6. (a) J. Sirker, A. Herzog, A. Oles y P. Horsch. *Phys. Rev. Lett.* 101, 2008, pág. 157204; (b) A. Herzog, P. Horsch, A. Oles y J. Sirker. *Phys. Rev. B* 84, 2011, pág. 134428.
7. (a) C. Lamas y J. Matera. *Phys. Rev. B* 92, 2015, pág. 115111; (b) J. Matera y C. Lamas. *J. Phys.: Condens. Matter* 26, 2014, pág. 326004.
8. D. Deutsch. «Quantum theory, the Church-Turing Principle and the universal quantum computer». *Proc. R. Soc. Lond. A* 400, 1985, pág. 97.
9. P. Shor. «Algorithms for Quantum Computation: Discrete Logarithms and Factoring». *Proc. Ann. Symp. Found. Comp. Science, IEEE Press, Ca.* 35, 1994, pág. 29.
10. L. Grover. «Quantum Mechanichs Helps in Searching for a Needle in a Haystack». *Phys. Rev. Lett.* 79, 1997, pág. 325.
11. M. A. Nielsen e I. L. Chuang. *Quantum Computation and Quantum Information*. 2000.
12. S. Aaronson y A. Arkhipov. «A Universal Training Algorithm for Quantum Deep Learning». *Proceedings of the forty-third annual ACM symposium on Theory of computing*, 2011, págs. 333-342.

13. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres y W. K. Wootters. «Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels». *Phys. Rev. Lett.* 70:13, 1993, págs. 1895-1899. DOI: 10.1103/PhysRevLett.70.1895.

14. E. Schrödinger. «Discussion of Probability Relations Between Separated Systems». *Proc. Cambridge Philos. Soc.* 31, 1935. ibid, 32, 446 (1936), págs. 555-563.

15. G. Vidal. «Entanglement renormalization.» *Phys. Rev. Lett.*, 2007, 99:220405.

16. B. Schumacher. «Quantum coding». *Phys. Rev. A* 51, 4 1995. C.H. Bennett, H. Bernstein, S. Popescu and B. Schumacher, Phys. Rev. **A 53** 2046 (1996), págs. 2738-2747. DOI: 10.1103/PhysRevA.51.2738. URL: http://link.aps.org/doi/10.1103/PhysRevA.51.2738.

17. C. H. Bennett, D. P. DiVincenzo, J. A. Smolin y W. K. Wootters. «Mixed-state entanglement and quantum error correction». *Phys. Rev. A* 54:5, 1996, págs. 3824-3851. DOI: 10.1103/PhysRevA.54.3824.

18. A. Wehrl. «General properties of entropy». *Rev. Mod. Phys.* 50, 2 1978, págs. 221-260. DOI: 10.1103/RevModPhys.50.221. URL: http://link.aps.org/doi/10.1103/RevModPhys.50.221.

19. J. von Neumann. «Wahrscheinlichkeitstheoretischer Aufbau der Quantenmechanik». *Göttinger Nachrichten*, 1927, pág. 245.

20. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres y W. K. Wootters. «Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels». *Phys. Rev. Lett.* 70, 13 1993, págs. 1895-1899. DOI: 10.1103/PhysRevLett.70.1895. URL: http://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

21. R. F. Werner. «Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model». *Phys. Rev. A* 40:8, 1989, págs. 4277-4281. DOI: 10.1103/PhysRevA.40.4277.

22. R. Rossignoli y C. T. Schmiegelow. «Entanglement generation resonances in XY chains». *Phys. Rev. A* 75:1, 2007, pág. 012320. DOI: 10.1103/PhysRevA.75.012320.

23. F. Giraldi y P. Grigolini. «Quantum entanglement and entropy.» *Phys. Rev. A* 64:2, 2001, pág. 032310.

24. A. Peres. «Separability Criterion for Density Matrices». *Phys. Rev. Lett.* 77:8, 1996, págs. 1413-1415. DOI: 10.1103/PhysRevLett.77.1413.

25. M. Horodecki, P. Horodecki y R. Horodecki. «Separability of mixed states: necessary and sufficient conditions». *Physics Letters A* 223:1-2, 1996, págs. 1-8. ISSN: 0375-9601. DOI: http://dx.doi.org/10.1016/S0375-9601(96)00706-2. URL: http://www.sciencedirect.com/science/article/pii/S0375960196007062.

26. N. Canosa y R. Rossignoli. «Generalized nonadditive entropies and quantum entanglement». *Physical Review Letters* 88:17, 2002, págs. 1704011-1704014.

27. R. Rossignoli y N. Canosa. «Generalized entropic criterion for separability». *Phys. Rev. A* 66:4, 2002, pág. 042306. DOI: 10.1103/PhysRevA.66.042306.

28. M. A. Nielsen y J. Kempe. «Separable States Are More Disordered Globally than Locally». *Phys. Rev. Lett.* 86:22, 2001, págs. 5184-5187. DOI: 10.1103/PhysRevLett.86.5184.

29. S. Hill y W. Wootters. «Entanglement of a pair of quantum bits». *Phys. Rev. Lett.* 78, 1997, pág. 5022.

30. G. Vidal y R. Werner. *Phys. Rev. A* 65, 2002, pág. 032314.

31. K. Zyczkowski, P. Horodecki, A. Sanpera y M. Lewenstein. *Phys. Rev. A* 58, 1998, pág. 883.

32. K. Zyczkowski. *Phys. Rev. A* 60, 1999, pág. 3496.