

Mecánica Cuántica y Qubits

En computación cuántica los estados asociados a los qubits están dados por vectores en espacios complejos de Hilbert de dimensión finita. En particular serán sistemas compuestos por partes de *dos niveles* con estado descrito por un vector en un espacio de Hilbert 2-dimensional.

Ejemplos de sistemas cuánticos de 2 niveles:

- Un fotón que puede pasar por dos caminos distintos como se ve en la figura 1.

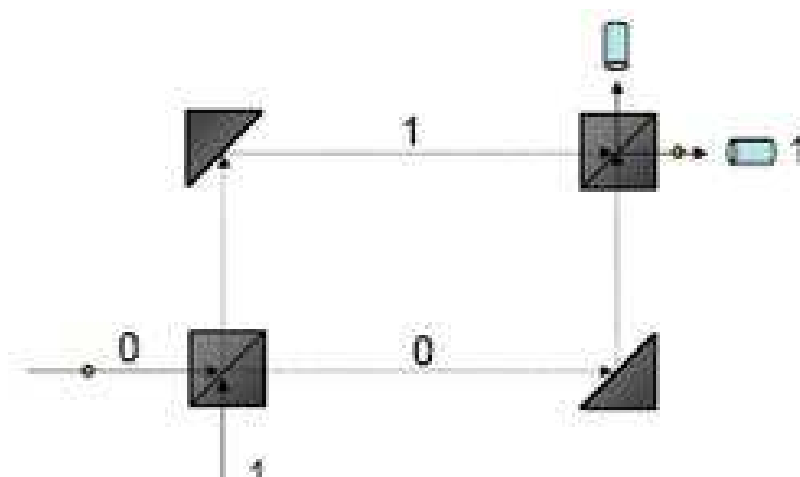


FIG. 1: Fotón que toma el camino $|0\rangle$ o el $|1\rangle$.

- Spin de las partículas de $spin -\frac{1}{2}$ como electrones, protones o neutrones. El spin estará *up* ($+\frac{1}{2}$) o *down* ($-\frac{1}{2}$).

- Energía de un electrón orbitando un núcleo como en el átomo de Hidrógeno. Sabemos que los posibles valores de energía son discretos o dicho de otra forma están cuantificados. El estado más probable es el *fundamental* seguido por el *primer excitado*. La probabilidad de que los otros estados estén ocupados es prácticamente despreciable así que se toma como un sistema de 2 niveles.

El estado de estos sistemas es descrito por un vector en un espacio de Hilbert de 2 dimensiones. Los estados asociados a cada uno de los niveles se identifican con $|0\rangle$ y $|1\rangle$ respectivamente.

El estado general del sistema será:

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle,$$

con α_0 y α_1 coeficientes complejos llamados las amplitudes de los estados de la base $|0\rangle$ y $|1\rangle$ respectivamente.

La condición de que el estado sea descrito por un vector unidad significa que $\alpha_0^2 + \alpha_1^2 = 1$. Esta condición es llamada *condición de normalización* y está asociada con el *proceso de medición* que veremos mas adelante. De esta forma el estado general del sistema será en cada uno de los ejemplos citados: la superposición de camino 0 y 1 para el fotón, del spin *up* y *down* para la partícula de *spin* $-\frac{1}{2}$ y del nivel fundamental y el excitado para el electrón en el átomo.

Fases en el vector de estado

Como la probabilidad de medición está asociada a la norma del vector de estado, el estado asociado a $e^{i\theta} |\psi\rangle$ es equivalente al asociado a $|\psi\rangle$. De forma que $|0\rangle + |1\rangle$ y $e^{i\theta} |0\rangle + e^{i\theta} |1\rangle$ se consideran equivalentes. Por otro lado *factores de fase relativos* entre estados ortogonales sí son significativos, de forma que el estado descrito por $|0\rangle + |1\rangle$ es físicamente distinto al de $|0\rangle + e^{i\theta} |1\rangle$.

Esfera de Bloch

El estado más general de un qubit se escribe de la forma:

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

que se representa como un punto en la superficie de una esfera 3-dimensional llamada *esfera de Bloch* como se ve en la figura 2.

Es interesante notar que el estado de un bit clásico que puede ser 0 o 1 se ubicaría en los polos norte y sur de la esfera de Bloch. Por otro lado si consideramos el caso probabilístico clásico que vimos en la introducción representado por

$$\begin{pmatrix} p_0 \\ p_1 \end{pmatrix}$$

se representaría como un punto sobre el segmento que une los polos verticalmente.

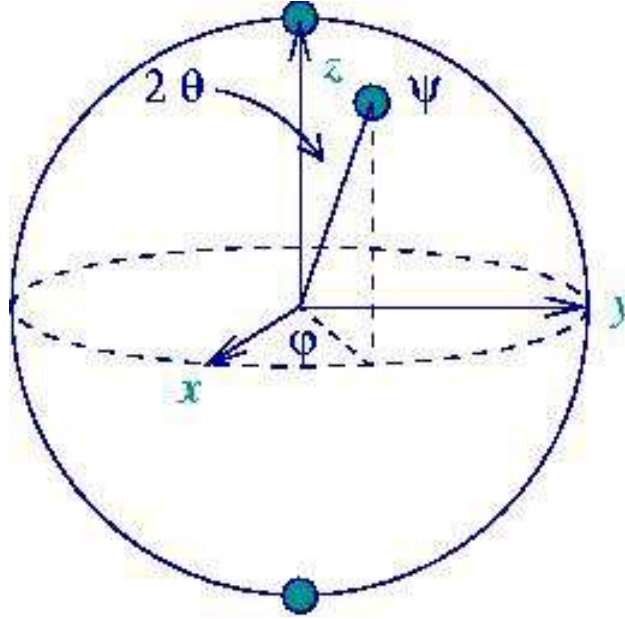


FIG. 2: Estado de qubit en la esfera de Bloch. (Donde dice 2θ debe decir θ)

A. Evolución en Sistemas Cerrados

Postulado de Evolución

La evolución temporal del estado de un sistema cuántico cerrado es descrita por un operador lineal unitario. Supongamos que el estado inicial es $|\psi_1\rangle$, después de la evolución será

$$|\psi_2\rangle = U |\psi_1\rangle .$$

Por linealidad se cumple que

$$U \sum_i \alpha_i |\psi_i\rangle = \sum_i \alpha_i U |\psi_i\rangle .$$

En computación cuántica podemos pensar a los operadores unitarios U que actúan sobre un solo qubit como *compuertas de 1-qubit*. De esta forma, como podemos representar los operadores sobre un qubit como matrices de 2×2 representados en una base. La compuerta cuántica *NOT*:

$$NOT : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

La matriz correspondiente será (en la base computacional):

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

La compuerta *NOT* se identifica con el símbolo *X* y es una de las *matrices de Pauli*:

$$\begin{aligned} \sigma_0 = I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \sigma_1 = \sigma_x = X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 = \sigma_y = Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, & \sigma_3 = \sigma_z = Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \end{aligned}$$

Veremos mas adelante que las compuertas de Pauli *X*, *Y* y *Z* corresponden a rotaciones alrededor de los ejes *x*, *y* y *z* de la esfera de Bloch, respectivamente. *Cualquier* operador unitario de 1-qubit se puede expresar como una combinación lineal de compuertas de Pauli.

Relación del Postulado de Evolución con la Ecuación de Schrödinger

La evolución de los sistemas cuánticos cerrados está dada por la *Ecuación de Schrödinger*

$$i\hbar \frac{d|\psi(t)\rangle}{dt} = H(t) |\psi(t)\rangle,$$

donde \hbar es la *constante de Planck* y $H(t)$ es un operador hermítico, el *Hamiltoniano* del sistema, que representa la Energía del mismo. Si consideramos Hamiltonianos constantes en el tiempo, la solución de la ecuación para dos tiempos t_1 y t_2 será:

$$|\psi(t_2)\rangle = e^{-i\hbar H(t_2-t_1)} |\psi(t_1)\rangle.$$

Ejercicio

Muestre que la anterior es solución de la Ecuación de Schrödinger con $H(t) = H$ constante en el tiempo.

Si H es hermítico $e^{-i\hbar H(t_2-t_1)}$ es unitario y así se verifica el Postulado de Evolución.

B. Sistemas Compuestos por muchos Qubits

Los problemas interesantes en computación cuántica tienen que ver con sistemas de varios qubits *que interactúan* entre sí. O sea que necesitamos saber cómo evoluciona un sistema con muchos qubits en el tiempo y qué pasa cuando lo medimos. Se trata a los sistemas grandes como composición de subsistemas lo que permite una descripción más eficiente de operaciones actuando sobre los subsistemas.

Postulado de Composición de Sistemas

Cuando dos sistemas físicos son tratados como un sistema, el espacio de estados de este sistema combinado es el espacio producto tensorial $\mathcal{H}_1 \otimes \mathcal{H}_2$ de los espacios de estados \mathcal{H}_1 , \mathcal{H}_2 de los subsistemas componentes. Si el primer sistema está en el estado $|\psi_1\rangle$ y el segundo en el estado $|\psi_2\rangle$, el estado del espacio combinado será:

$$|\psi_1\rangle \otimes |\psi_2\rangle.$$

Como dijimos antes este estado conjunto se escribe $|\psi_1\psi_2\rangle$.

Aplicando el Postulado de Composición de Sistemas inductivamente se puede deducir que el espacio de estados de n subsistemas es el producto tensorial de los espacios de estado de los n subsistemas.

Estados Enredados (Entangled)

Es importante señalar que el estado de un sistema compuesto de 2-qubits *no siempre puede* ser escrito en la forma $|\psi_1\rangle \otimes |\psi_2\rangle$. Un ejemplo importante en el que no se puede poner como producto tensorial es el de los estados *enredados* o *entangled* en el que los qubits no están aislados y pueden interactuar. De cualquier forma el estado del sistema compuesto es un vector en el espacio 4-dimensional producto tensorial de los espacios de los 2 qubits. Aquellos vectores que son el producto tensorial de dos vectores bidimensionales forman un subconjunto raro (sparse) del conjunto de todos los vectores del espacio 4-dimensional. Podemos decir entonces que la mayoría de los estados de 2-qubits son enredados.

Ejercicio

Considere el estado de 2-qubits:

$$|\psi\rangle = \frac{1}{\sqrt{2}} |0\rangle |0\rangle + \frac{1}{\sqrt{2}} |1\rangle |1\rangle.$$

Muestre que este estado es enredado probando que no hay ningún valor de $\alpha_0, \alpha_1, \beta_0, \beta_1$ tal que

$$|\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle)(\beta_0 |0\rangle + \beta_1 |1\rangle).$$

$|\psi\rangle$ es conocido como *par EPR* porque fue introducido por Einstein, Podolsky y Rosen en un artículo muy importante y controversial para la mecánica cuántica de 1935. Se volverá mas adelante sobre estos estados enredados que son de mucha importancia para la computación cuántica.

Supongamos que tenemos un sistema compuesto por 2 qubits y aplicamos la compuerta *NOT* (X) al primer qubit. Si no hacemos otra cosa, estamos implícitamente aplicando el operador identidad I al segundo qubit. De forma que la entrada de 2-qubits $|\psi_1\rangle \otimes |\psi_2\rangle$ se transforma en $X |\psi_1\rangle \otimes I |\psi_2\rangle = (X \otimes I)(|\psi_1\rangle \otimes |\psi_2\rangle)$. La representación matricial de $X \otimes I$ es:

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}.$$

Por más que actúa en un sistema de 2-qubits esta compuerta se considera *compuerta de 1-qubit* porque actúa *no trivialmente* sobre uno sólo de los qubits.

Si el sistema fuera de n qubits, aplicar X al primer qubit solamente corresponde a aplicar $X \otimes I \otimes I \cdots \otimes I$, con I repetido $n - 1$ veces, a todo el sistema. En forma matricial sería una matriz de $2^n \times 2^n$.

Así como hay estados de 2-qubits que no pueden ser escritos como producto de estados de 1-qubit, hay compuertas de 2-qubits que no pueden ser escritas como producto de compuertas de 1-qubit. Un ejemplo importante es la compuerta cuántica *controlled-NOT* o CNOT. En la base computacional la compuerta CNOT cambia el estado del segundo qubit si el primer qubit está en $|1\rangle$ y lo deja como está si no:

$$|00\rangle \rightarrow |00\rangle, |01\rangle \rightarrow |01\rangle, |10\rangle \rightarrow |11\rangle, |11\rangle \rightarrow |10\rangle.$$

Su representación matricial es:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Ejercicio

Verifique que la matriz atribuida a CNOT cambia el estado del segundo qubit si el primer qubit está en $|1\rangle$ y lo deja como está si no.

C. Medición

En el Postulado de Evolución se menciona la condición de que el sistema cuántico en cuestión sea *cerrado*, lo que significa que no hay interacción con su ambiente. Cuando se mide alguna de las propiedades de interés del sistema ya se pierde esa condición debido a que se produce la interacción entre el aparato de medición y el sistema y por lo tanto el Postulado de Evolución y su condición de unitariedad ya no se cumplen. El proceso de medición está descrito por el Postulado de Medición.

Postulado de Medición

Sea el estado del sistema A

$$|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle,$$

con $\{|\varphi_i\rangle\}$ una base ortonormal del espacio de estados \mathcal{H}_A del sistema. Una *medición de Von Neumann* sobre el sistema A con respecto a la base $\{|\varphi_i\rangle\}$ tendrá como resultado i con probabilidad $|\alpha_i|^2$ dejando a A en el estado $|\varphi_i\rangle$. El resultado i es lo que marca el aparato de medición.

Si consideramos un espacio de estados bipartito $\mathcal{H}_A \otimes \mathcal{H}_B$ y el sistema en el estado

$|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle |\gamma_i\rangle$, la medición sobre A tendrá como resultado i con probabilidad α_i^2 dejando al sistema bipartito en el estado $|\varphi_i\rangle |\gamma_i\rangle$.

Ejercicio

De acuerdo al Postulado de Medición la probabilidad de obtener i es $p(i) = |\alpha_i|^2$ si el estado del sistema es $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle$, con $|\alpha_i|^2 = \alpha_i \alpha_i^* = \langle \psi | \varphi_i \rangle \langle \varphi_i | \psi \rangle$. Muestre que los estados $|\psi\rangle$ y $e^{i\theta} |\psi\rangle$ son equivalentes dado que $p(i)$ es la misma en ambos casos. Ésta es la justificación de que las fases globales no tengan significado físico.

Medición Proyectiva

La medición de Von Neumann es una clase especial de *medición proyectiva*. Habíamos visto que una proyección ortogonal es un operador P que cumple $P^\dagger = P$ y $P^2 = P$. Para una descomposición del operador identidad $I = \sum_i P_i$ en proyectores ortogonales P_i , existe una medición proyectiva con salida i , con probabilidad $p(i) = \langle \psi | P_i | \psi \rangle$ y que deja al sistema en el estado $\frac{P_i |\psi\rangle}{\sqrt{p(i)}}$. En otras palabras esta medición proyecta el estado inicial $|\psi\rangle$ con uno de los proyectores posibles P_i con probabilidad igual al cuadrado del módulo de la amplitud de la componente de $|\psi\rangle$ en el subespacio de la proyección.

Ejercicio

- Pruebe que si los operadores proyección P_i satisfacen $P_i^\dagger = P_i$ y $P_i^2 = P_i$, entonces $P_i P_j = 0 \quad \forall i \neq j$.
- Pruebe que todo estado $|\psi\rangle$ puede ser descompuesto como $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$ donde $\alpha_i = \sqrt{p(i)}$, $p(i) = \langle \psi | P_i | \psi \rangle$ y $|\psi_i\rangle = \frac{P_i |\psi\rangle}{\sqrt{p(i)}}$. Pruebe también que $\langle \psi_i | \psi_j \rangle = \delta_{i,j}$.
- Pruebe que cualquier descomposición $I = \sum_i P_i$ del operador identidad en un espacio de Hilbert de dimensión N tiene a lo sumo N términos en la suma.

La medición de Von Neumann se caracteriza por ser *completa* o máxima porque los proyectores P_i que participan en la misma cumplen con la condición de completitud $I = \sum_i P_i$. Un ejemplo simple de medición de Von Neumann es una medición en la base computacional en la que los proyectores $P_i = |i\rangle \langle i|$ proyectan sobre los vectores base y se cumple completitud. Un ejemplo de medición proyectiva *incompleta* es una medición de paridad, donde $P_0 = \sum_{parity(x)=0} |x\rangle \langle x|$ y $P_1 = \sum_{parity(x)=1} |x\rangle \langle x|$, o sea que en P_0 se suman todas las secuencias

con un número par de 1s y en P_1 aquellos con número impar de 1s.

Las mediciones proyectivas son frecuentemente descritas en términos de un *observable*. Todo observable en cuántica es un operador Hermítico M que actúa en el espacio de estados del sistema. Dado que M es Hermítico tiene una descomposición espectral

$$M = \sum_i m_i P_i$$

donde P_i es el proyector ortogonal sobre el autoespacio de M con autovalor real m_i . Medir el observable M se entiende como realizar una medición proyectiva con respecto a la descomposición $I = \sum_i P_i$ donde la medición correspondiente a i es el autovalor m_i .

Ejercicio

Considere el operador de Pauli Z :

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Dado que Z es hermítico puede ser (y de hecho es) un observable.

- Expresar la descomposición espectral de Z en la base computacional.
- Cuáles serían los resultados posibles de una medición?

Ejercicio

Verifique que la medición del observable de Pauli X es equivalente a una medición proyectiva completa con respecto a la base $\{|+\rangle, |-\rangle\}$

Ejercicio

- Pruebe que la realización de una medición proyectiva de Paridad con respecto a P_0 y P_1 sobre un estado de n -qubits es equivalente a medir el observable $Z^{\otimes n}$.
- Explique por qué no es equivalente realizar una operación completa de Von Neumann con respecto a la base computacional y luego medir la paridad de la cadena resultante a hacer directamente una medición proyectiva de la paridad.

Ejercicio

Imagine un experimento en el que no se miden sistemas cuánticos individuales sino un con-

junto de sistemas igualmente preparados e independientes y en el que el aparato de medición da un promedio sobre los valores posibles m_i llamado *valor esperado*: $M = \sum_i p(i)m_i$. Considere una medición proyectiva descrita por proyectores P_i y se mide el estado $|\psi\rangle$. Demuestre que

$$M = \text{Tr}(M |\psi\rangle \langle\psi|)$$

Medición POVM

El Postulado de Medición da por un lado las probabilidades de las diferentes mediciones posibles y por el otro el estado en el que queda el sistema después de la medición. En algunos casos el estado del sistema después no es importante, importando las probabilidades de las mediciones solamente. Por ejemplo si el sistema es medido sólo una vez. En estos casos se usa el *formalismo POVM*. POVM es por Positive Operator-Valued Measure.

Supongamos que los operadores de medición son M_m y el estado del sistema es $|\psi\rangle$. La probabilidad de que se mida m es: $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$. Si definimos:

$$E_m = M_m^\dagger M_m$$

. E_m es un operador positivo que cumple que $\sum_m E_m = I$ y $p(m) = \langle\psi|E_m|\psi\rangle$. El conjunto de operadores $\{E_m\}$ son suficientes para determinar las probabilidades. Los operadores E_m son los *elementos POVM* de la medición.

Ejemplo de POVM

Medición proyectiva con operadores P_m tales que $P_m P_{m'} = \delta_{mm'}$ y $\sum_m P_m = I$. En este ejemplo (y sólo en él) los elementos POVM son los operadores de medición porque $E_m = P_m^\dagger P_m = P_m$.

D. Estados Mixtos y Matriz Densidad

Hasta ahora se ha considerado que el sistema está en un estado definido que se conoce como *estado puro*. Sin embargo, hay casos en los que los qubits están asociados a un *conjunto* de estados posibles con sus respectivas probabilidades (que suman 1). Por ejemplo, el qubit

está en el estado puro $|\psi_1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ con probabilidad $1/3$ y en el estado puro $|\psi_2\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ con probabilidad $2/3$. El estado descrito por esta distribución de probabilidad se llama *mezcla* o *ensemble* de los estados $|\psi_1\rangle$ y $|\psi_2\rangle$. El estado correspondiente se llama *estado mixto*.

Una forma de representar un estado mixto general en n qubits es como el conjunto:

$$\{(|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \dots, (|\psi_k\rangle, p_k)\}$$

lo que significa que la probabilidad de que el sistema esté en el estado puro $|\psi_1\rangle$ es p_1 , etc. hasta k . Un estado puro puede ser considerado como mixto con todos salvo uno de los p nulos.

La alternativa mas usada para describir estados mixtos es en términos de operadores llamados *operadores densidad* con sus correspondientes *matrices densidad*.

El operador densidad para un estado puro $|\psi\rangle$ está definido por:

$$\rho = |\psi\rangle \langle\psi|.$$

Si aplicamos el operador unitario U al estado $|\psi\rangle$ se obtiene el estado $U|\psi\rangle$ con operador densidad $U|\psi\rangle \langle\psi| U^\dagger$. Supongamos que medimos el estado dado por $\rho = |\psi\rangle \langle\psi|$ en la base computacional. La probabilidad de obtener 0 es:

$$\langle 0|\psi\rangle \langle\psi|0\rangle = \langle 0|\rho|0\rangle$$

esta probabilidad es un número real que puede ser considerado como la traza de una matriz de 1×1 con ese mismo número como componente, por lo tanto:

$$\langle 0|\psi\rangle \langle\psi|0\rangle = Tr(\langle 0|\psi\rangle \langle\psi|0\rangle) = Tr(|0\rangle \langle 0|\psi\rangle \langle\psi|)$$

El último paso se debe a que la traza es cíclica : $Tr(ABC) = Tr(BCA) = Tr(CAB)$. De igual forma la probabilidad de obtener 1 será $Tr(|1\rangle \langle 1|\psi\rangle \langle\psi|)$

El operador densidad para el estado mixto general referido antes es:

$$\rho = \sum_{i=1}^k p_i |\psi_i\rangle \langle\psi_i|.$$

y contiene toda la información relevante sobre el estado del sistema.

Si se aplica el operador U a este estado mixto el operador densidad resultante es:

$$\sum_{i=1}^k p_i U |\psi_i\rangle \langle \psi_i| U^\dagger = U \left(\sum_{i=1}^k p_i |\psi_i\rangle \langle \psi_i| \right) U^\dagger = U \rho U^\dagger$$

La probabilidad de obtener 0 si se mide en la base computacional será en este caso:

$$\begin{aligned} \sum_i p_i \text{Tr}(|0\rangle \langle 0| \psi_i\rangle \langle \psi_i|) &= \text{Tr}(\sum_i p_i |0\rangle \langle 0| \psi_i\rangle \langle \psi_i|) \\ &= \text{Tr}(|0\rangle \langle 0| \sum_i p_i |\psi_i\rangle \langle \psi_i|) = \text{Tr}(|0\rangle \langle 0| \rho). \end{aligned}$$

Para calcular la estadística asociada con la medida de algún observable de un sistema, lo único que importa es el operador densidad y no la descomposición del mismo. En otras palabras, dos mezclas distintas que tengan las mismas matrices densidad son indistinguibles o equivalentes.

Ejercicio

Encuentre las matrices densidad de los siguientes conjuntos:

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

Ejercicio

a) Pruebe que el operador densidad ρ satisface:

$$\text{Tr}(\rho) = 1$$

ρ es un operador positivo (para todo $|v\rangle$, $\langle v|\rho|v\rangle$ es real y no-negativo, o lo que es equivalente que los autovalores de ρ son no-negativos).

Ejercicio

Considere una transformación lineal T en un espacio de Hilbert \mathcal{H} de dimensión N . Esta transformación T produce una transformación $\rho \rightarrow T\rho T^\dagger$. Pruebe que esta última transformación es también lineal.