Computación Cuántica

La medición en sistemas de múltiples cúbits

Índice

Esquema 2

Ideas clave 3

5.1 Introducción y objetivos 3

5.2 Transformaciones lineales 4

5.3 Referencias bibliográficas 23

Esquema

La medición en los sistemas cuánticos de múltiples cúbits

Transformaciones lineales

- Notación bra-ket
- Operador de proyección
- Observables
- Operador adjunto
- Operador hermítico

Postulado de medida

Medición de estados entrelazados

5.1 Introducción y objetivos

Dado un estado desconocido de un cúbit $|\Psi\rangle$, no es posible, experimentalmente, conocer ese estado, el estado cuántico no es directamente observable, solo podemos acceder a los resultados de las mediciones que realicemos sobre él.

La siguiente figura muestra como la luz del sol proyecta una sombra sobre el suelo, la esfera no es *observable*, en esta analogía, pero su proyección nos da cierta información sobre ella. Además vemos como un objeto de tres dimensiones al ser proyectado, se reduce a un objeto de dos dimensiones, el proceso de proyección tiene esa característica de reducir la dimensión. El operador de proyección proyecta uno estado cuántico en otro, es una herramienta que tiene aplicación en muchas situaciones en mecánica cuántica, como en el caso de medir la propiedad de un partícula, al hacerlo, su estado (esfera) colapsa a otro estado diferente (sombra). El operador de proyección permite describir matemáticamente este colapso.

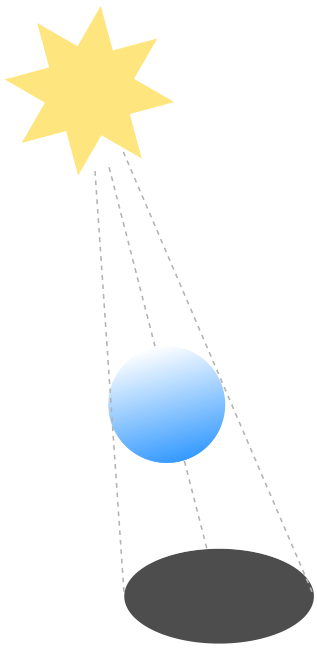

Figura 1: Sombra proyectada por una esfera. Elaboración propia.

En temas anteriores se estudió el producto interno o producto escalar, como un operador que actúa sobre un vector para proporcionar un escalar, ahora podemos describir otro operador, extendiendo la idea de producto escalar, para definir una transformación lineal de proyección que actúa sobre un vector para producir otro vector.

La medida del estado de un sistema cuántico muestra un comportamiento no clásico y tiene una importancia fundamental en computación cuántica. Este tema trata sobre el formalismo utilizado para la medición de los sistemas de múltiples cúbits y como aplicarlo para entender el comportamiento altamente no clásico de los estados entrelazados bajo el proceso de medida. Se comienza por extender la notación de Dirac a las transformaciones lineales ya que será utilizada para describir las medidas y las transformaciones que actúan sobre los sistemas cuánticos. Se trabaja con los operadores de proyección, el concepto de observable y el postulado de medida. Finalmente se estudia el comportamiento bajo medición de los estados entrelazados.

- La medición en sistemas de múltiples cúbits
- Transformaciones lineales
- El operador de proyección
- Observables
- Operador adjunto
- Operador hermítico
- El Postulado de medida
- Medición de estados entrelazados

5.2 Transformaciones lineales

En computación clásica utilizamos números y funciones, en computación cuántica utilizaremos vectores y transformaciones lineales.

Computación clásica			Computación cuántica	
Números	x	→	Vectores	|x>
Funciones	f(x)		Transformaciones lineales	Ô|x>

Figura 2: Computación cuántica y clásica. Elaboración propia.

La notación de Dirac o también conocida como notación bra-ket, proporciona una forma intuitiva y conveniente de expresar las transformaciones lineales que actúan sobre los estados cuánticos. Un vector columna se representa mediante un ket $|\psi\rangle$ y su transpuesto conjugado mediante el bra $\langle\psi|$. El producto escalar de dos vectores se expresa de la forma $\langle\psi|\varphi\rangle$ y el producto externo como $|\psi\rangle\langle\varphi|$.

La multiplicación de matrices es asociativa y los escalares se conmutan con todo, y por tanto se cumplen las siguientes expresiones:

$$(|a\rangle\langle b|)|c\rangle = |a\rangle(\langle b||c\rangle) = (\langle b|c\rangle)|a\rangle$$

Sea V un espacio vectorial asociado con un sistema de un solo cúbit. La matriz para el operador$|0\rangle\langle 0|$ con respecto a la base estándar en el orden estándar $|0\rangle, |1\rangle$ es la siguiente:

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

Y la matriz para el operador$|1\rangle\langle 1|$ con respecto a la base estándar es la siguiente:

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

La notación $|0\rangle\langle 1|$ representa la transformación lineal que asigna el estado $|1\rangle$ con el $|0\rangle$ y el estado$|0\rangle$ con el vector nulo, una relación sugerida de forma intuitiva por la notación siguiente:

$$(|0\rangle\langle 1|)|1\rangle = |0\rangle(\langle 1|1\rangle) = |0\rangle(1) = |0\rangle,$$

$$(|0\rangle\langle 1|)|0\rangle = |0\rangle(\langle 1|0\rangle) = |0\rangle(0) = 0$$

De forma semejante:

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

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

Y por lo tanto, todas las transformaciones lineales de dos dimensiones en V se pueden escribir utilizando esta notación:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = a|0\rangle\langle 0| + b|0\rangle\langle 1| + c|1\rangle\langle 0| + d|1\rangle\langle 1|$$

De este modo, la transformación lineal que intercambia los estados $|0\rangle$ y $|1\rangle$ es la siguiente:

$$X = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Que también se puede expresar de la siguiente forma, especificando la transformación lineal en términos de su efecto sobre los vectores de la base:

X :

$|0\rangle \mapsto |1\rangle$

$|1\rangle \mapsto |0\rangle$

La transformación $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ se representa también con respecto a la base computacional como la siguiente matriz:

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

La siguiente figura muestra el efecto de la transformación X sobre distintos estados:

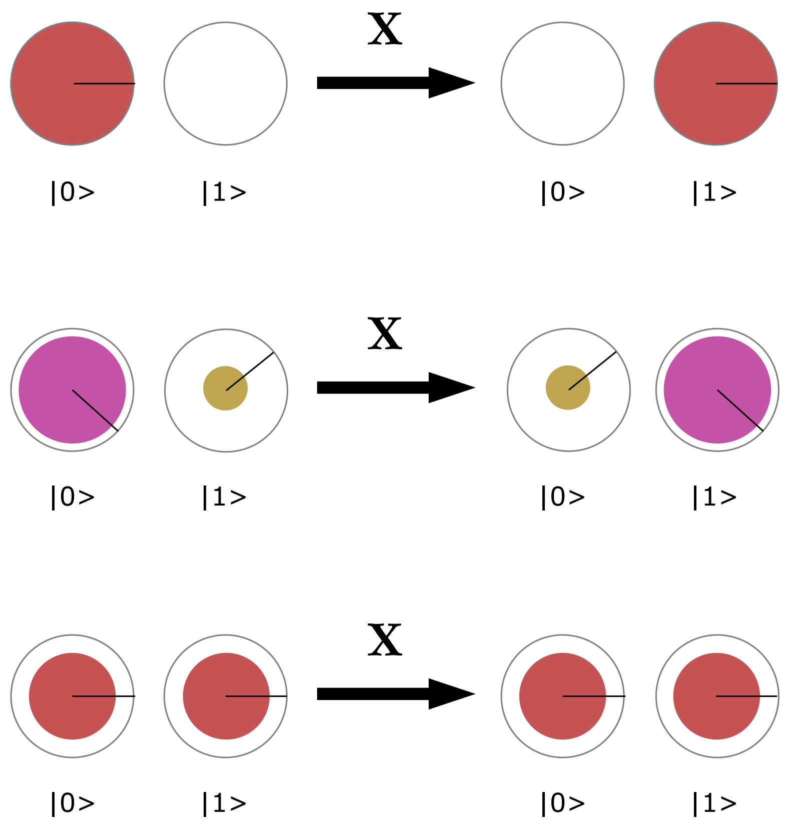

Figura 3: Efecto de la transformación X sobre distintos estados. Elaboración propia.

Así, por ejemplo, para un sistema de dos cúbits, la transformación que intercambia los vectores $|00\rangle$ y $|10\rangle$, y no modifica el resto de estados, se expresa como:

$$|10\rangle\langle 00| + |00\rangle\langle 10| + |11\rangle\langle 11| + |01\rangle\langle 01|$$

Y su correspondiente representación matricial, en la base computacional o base estándar, sería:

$$\begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

El proyector, u operador de proyección

Dado un estado desconocido de un cúbit $a|0\rangle + b|1\rangle$, no es posible experimentalmente conocer ese estado, el estado cuántico no es directamente observable. Solo podemos acceder a los resultados de las mediciones y por ello, los operadores hermíticos que utilizamos para realizar la medición, se denominan *observables*.

La siguiente figura muestra los resultados de realizar la medida, con respecto de la base computacional, de un cúbit que se encuentra en diferentes estados.

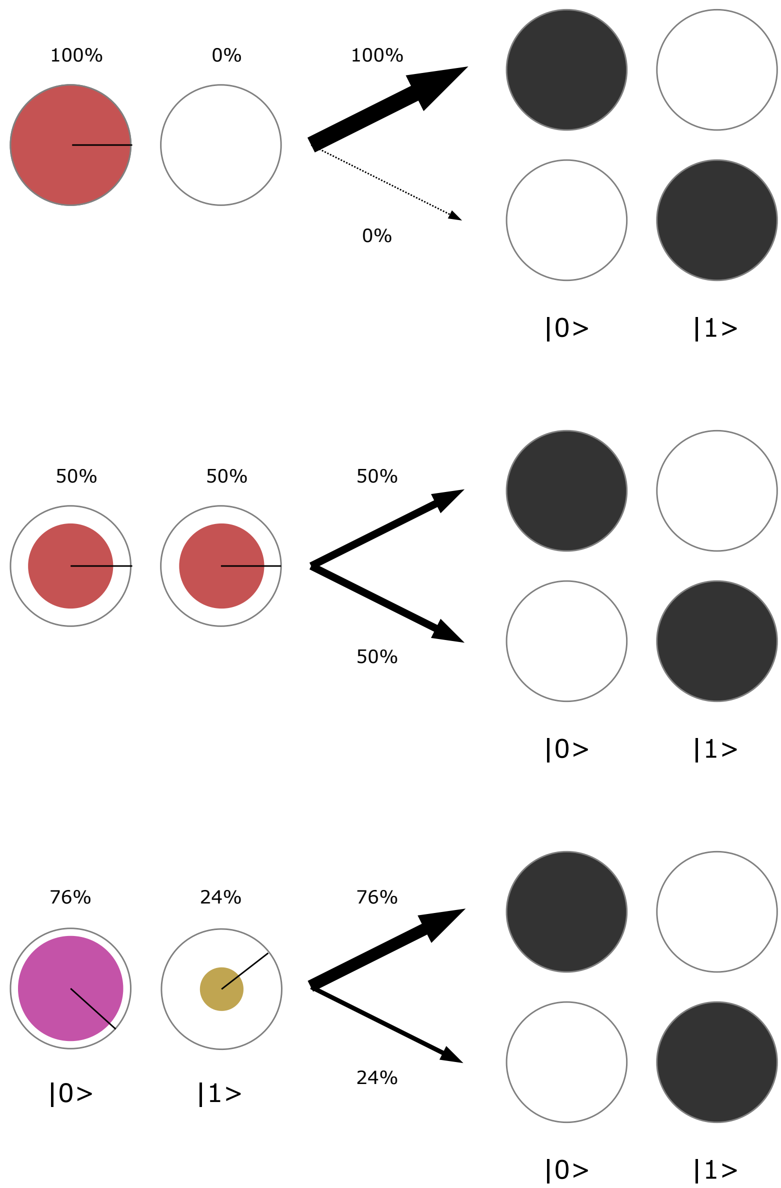

Figura 4: Resultados de mediciones en la base computacional. Elaboración propia.

Se puede escribir un operador, en un sistema de n cúbits, que asigna el vector base $|j\rangle$ al vector $|i\rangle$ y todos los demás vectores de la base computacional a 0 como:

$\hat{O} = |i\rangle\langle j|$

La matriz correspondiente al operador $\hat{O}$ tiene una única entrada distinta de cero en el elemento ij. Se puede escribir un operador general $\hat{O}$ con entradasa_{ij} en la base computacional como:

$$\hat{O} = \sum_i \sum_j a_{ij}|i\rangle\langle j|$$

De forma semejante, el elemento ij de la matriz $\hat{O}$, en la base computacional, puede expresarse como: $\langle i|\hat{O}|j\rangle$

Si aplicamos el operador $\hat{O}$ a un estado genérico $|\psi\rangle = \sum_k b_k|k\rangle$ se obtendría:

$$\hat{O}|\psi\rangle = (\sum_i \sum_j a_{ij}|i\rangle\langle j|)(\sum_k b_k|k\rangle) = \sum_i \sum_j \sum_k a_{ij}b_k|i\rangle\langle j||k\rangle = \sum_i \sum_j a_{ij}b_j|i\rangle$$

De esta forma, si $\hat{O}$ es el operador que asigna $|10\rangle$ a $|11\rangle$y $|11\rangle$ a $|10\rangle$:

$$\hat{O} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| = \sum_i \sum_j a_{ij}|i\rangle\langle j|$$

donde:

$a_{00} = 1, a_{01} = 0, a_{02} = 0, a_{03} = 0, a_{10} = 0, a_{11} = 1, a_{12} = 0, a_{13} = 0, a_{20} = 0, a_{21} = 0, a_{22} = 0, a_{23} = 1, a_{30} = 0, a_{31} = 0, a_{32} = 1, a_{33} = 0$

Al actuar sobre el estado: $|\psi\rangle = \sum_k b_k|k\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

donde:

$b_0 = \frac{1}{2}, b_1 = \frac{1}{2}, b_2 = \frac{1}{2}, b_3 = \frac{1}{2}$

$$\hat{O}|\psi\rangle = (\sum_i \sum_j a_{ij}|i\rangle\langle j|)(\sum_k b_k|k\rangle)$$

Por tanto:

$$\hat{O}|\psi\rangle = \sum_i \sum_j \sum_k a_{ij}b_k|i\rangle\langle j||k\rangle = \sum_i \sum_j a_{ij}b_j|i\rangle$$

Puesto que $\langle j||k\rangle = 0$ siempre que $j \neq k$ al ser los vectores de la base ortogonales, finalmente:

$$\hat{O}|\psi\rangle = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|)\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

De forma general, si $|\beta_0, \beta_1, ..., \beta_{N-1}\rangle$ es una base del espacio vectorial V de dimensión N, entonces, un operador $\hat{O} : V \mapsto V$ puede expresarse, con respecto a esa base, como:

$\hat{O} = \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} b_{ij} |\beta_i\rangle\langle\beta_j|$

En concreto, la matriz correspondiente al operador $\hat{O}$ con respecto de la base $|\beta_0, \beta_1, ..., \beta_{N-1}\rangle$, tiene entradas: $O_{ij} = b_{ij}$

La notación matricial puede resultar más familiar y fácil de comprender inicialmente y es conveniente para realizar cálculos. Sin embargo, exige elegir una base y un orden en los vectores que forman esa base. La notación de Dirac es independiente de la base así como del orden de los elementos que la forman. También resulta más compacta e intuitiva, sugiriendo las relaciones correctas, como en el caso del producto exterior.

Operadores de proyección para la medida

La idea introducida en temas anteriores de realizar la medida de un sistema de un cúbit mediante la proyección sobre uno de los vectores de la base asociado con el dispositivo de medida, puede generalizarse para realizar la medida en sistemas de múltiples cúbits.

Para cualquier subespacio S de V, el subespacio $S^\perp$ está formado por todos los vectores que son perpendiculares a los vectores en S. Los subespacios S y $S^\perp$ satisfacen $V = S \oplus S^\perp$ y por lo tanto, cualquier vector $|v\rangle \in V$ se puede escribir únicamente como la suma de un vector $\vec{s}_1 \in S$ y un vector $\vec{s}_2 \in S^\perp$. Para cualquier S, el operador de proyección P_S es el operador lineal $P_S : V \mapsto S$ que envía $|v\rangle \mapsto \vec{s}_1$ donde $|v\rangle = \vec{s}_1 + \vec{s}_2$ con $\vec{s}_1 \in S$ y $\vec{s}_2 \in S^\perp$. Utilizamos la notación $\vec{s}_i$ porque $\vec{s}_1$ y $\vec{s}_2$, por lo general, no son vectores unitarios. El operador $|\psi\rangle\langle\psi|$ es el operador de proyección en el subespacio generado por $|\psi\rangle$. Los operadores de proyección a veces se denominan *proyectores* para abreviar. Para cualquier descomposición de suma directa de $V = S_1 \oplus \cdots \oplus S_k$ en subespacios ortogonales S_i existen k operadores de proyección relacionados $P_i : V \rightarrow S_i$ donde $P_i|v\rangle = \vec{s}_1$ siendo $|v\rangle = \vec{s}_1 + ... + \vec{s}_k$ con $s_i \in S_i$.

Siguiendo la terminología anteriormente descrita, un dispositivo de medición con una descomposición asociada $V = S_1 \oplus \cdots \oplus S_k$ que actúa sobre un estado $|\psi\rangle$ da como resultado, con probabilidad: $|P_i|\psi\rangle|^2$, el siguiente estado:

$$|\varphi\rangle = \frac{P_i|\psi\rangle}{|P_i|\psi\rangle|}$$

De esta forma, el proyector $|0\rangle\langle 0|$ aplicado a un estado $|\psi\rangle$ de un cúbit proporciona la componente de $|\psi\rangle$ en el subespacio generado por $|0\rangle$. Si $|\psi\rangle = a|0\rangle + b|1\rangle$, entonces:

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

De igual forma, el operador $|1\rangle|0\rangle\langle 1|\langle 0|$, que actúa sobre estados de dos cúbits, aplicado al estado genérico:

$$|\varphi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

proporciona:

$$(|1\rangle|0\rangle\langle 1|\langle 0|)|\varphi\rangle = (|10\rangle\langle 10|)(a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle) = a_{10}|10\rangle.$$

Si P_S es el operador de proyección de un espacio vectorial V de dimensión n en un subespacio S de dimensión s con una base $|\beta_0, \beta_1, \ldots, \beta_{S-1}\rangle$, entonces:

$$P_S = \sum_{i=1}^{S-1} |\beta_i\rangle\langle\beta_i| = |\beta_0\rangle\langle\beta_0| + \ldots + |\beta_{s-1}\rangle\langle\beta_{s-1}|$$

Por lo tanto, si:

$$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

representa el estado de un sistema de dos cúbits con un espacio vectorial asociado V, entonces, si S_1 es el subespacio generado por los vectores $|00\rangle$, $|01\rangle$, el operador de proyección $P_S = |00\rangle\langle 00| + |01\rangle\langle 01|$ es el proyector que transforma $|\psi\rangle$en el vector, no normalizado:

$$|\psi'\rangle = a_{00}|00\rangle + a_{01}|01\rangle$$

Operador adjunto

Sean V y W dos espacios vectoriales con producto interno. El operador adjunto o transpuesto conjugado $O^\dagger : V \to W$ de un operador $O : W \to V$ se define como el operador que satisface la siguiente relación de producto interno. Para cualquier $\vec{v} \in V$ y $O\vec{w} \in W$, el producto interno entre $O^\dagger\vec{v}$ y $\vec{w}$ es el mismo que el producto interno entre e $\vec{v}$ y $O^\dagger\vec{w}$:

$$O^\dagger\vec{v}\cdot\vec{w} = \vec{v}\cdot O\vec{w}$$

La matriz correspondiente al operador adjunto $O^\dagger$ de O se obtiene tomando el complejo conjugado de todos los elementos y luego la transpuesta, donde se asume el uso consistente de las bases para V y W.

Utilizando la notación de Dirac, la relación entre el producto interno de $O^\dagger|x\rangle$ y $|w\rangle$ y el producto interno entre $|x\rangle$ y $O|w\rangle$ queda reflejado en la notación:

$$(\langle x|O)|w\rangle = \langle x|(O|w\rangle) = \langle x|O|w\rangle$$

Por la propia definición del operador de proyección P se deduce que aplicar un operador de proyección varias veces seguidas tiene el mismo efecto que aplicarlo una sola vez:

$$PPP = PP = P$$

Además, cualquier operador de proyección es su propio adjunto:

$$P = P^\dagger$$

Por lo tanto $|P|v\rangle|^2 = (\langle v|P^\dagger)(P|v\rangle) = \langle v|P|v\rangle$ para cualquier operador de proyección P y todo $|v\rangle \in V$.

Se utiliza a continuación la notación de Dirac para describir la medición de un sistema de un cúbit en la base computacional siguiendo este formalismo.

Sea V el espacio vectorial asociado con un sistema de un solo cúbit. La descomposición de suma directa para V asociada con la medición en la base estándar es $V = S \oplus S'$, donde S es el subespacio generado por $|0\rangle$ y S' es el subespacio generado por $|1\rangle$. Los operadores de proyección correspondientes son $P : V \to S$ y $P' : V \to S'$, donde:

$$P = |0\rangle\langle 0| \text{ y}$$

$$P' = |1\rangle\langle 1|$$

La medida del estado $|\psi\rangle = a|0\rangle + b|1\rangle$ da como resultado el estado $\frac{P|\psi\rangle}{|P|\psi\rangle|}$ con probabilidad $|P|\psi\rangle|^2$. Ya que:

$P|\psi\rangle = (|0\rangle\langle 0|)|\psi\rangle = |0\rangle\langle 0|\psi\rangle = a|0\rangle$ y

$|P|\psi\rangle|^2 = \langle\psi|P|\psi\rangle = \langle\psi|(|0\rangle\langle 0|)|\psi\rangle = \langle\psi|0\rangle\langle 0|\psi\rangle = aa = |a|^2$,

el resultado de la medición es $\frac{a|0\rangle}{|a|}$ con probabilidad $|a|^2$. Dado que, la fase global carece de significado físico, el estado $|0\rangle$ se ha obtenido con probabilidad $|a|^2$y de la misma forma, el estado representado por $|1\rangle$ se obtiene con probabilidad $|b|^2$.

Veamos ahora la medida de un sistema de dos cúbits con respecto a la descomposición correspondiente a la base estándar.

Sea V el espacio vectorial asociado con un sistema de dos cúbits y $|\varphi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ un estado arbitrario de dos cúbits. Veamos la medida de este sistema con la descomposición $V = S_{00} \oplus S_{01} \oplus S_{10} \oplus S_{11}$, donde S_{ij} es el subespacio complejo de una dimension generado por $|ij\rangle$.Los operadores de proyección correspondientes $P_{ij} : V \to S_{ij}$ son:

$P_{00} = |00\rangle\langle 00|$

$P_{01} = |01\rangle\langle 01|$

$P_{10} = |10\rangle\langle 10|$

$P_{11} = |11\rangle\langle 11|$

El estado, tras realizar la medida será por tanto: $\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|}$ con probabilidad $|P_{ij}|\psi\rangle|^2$.

Puesto que dos vectores$|v\rangle$ and $|w\rangle$ representan el mismo estado cuando $|v\rangle = e^{i\theta}|w\rangle$, entonces, el estado tras realizar la medida será uno de los cuatro posibles resultados siguientes::

$\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|} = \frac{a_{00}|00\rangle}{|a_{00}|} \sim |00\rangle$ con probabilidad $\langle\psi|P_{00}|\psi\rangle = |a_{00}|^2$

$\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|} = \frac{a_{01}|01\rangle}{|a_{01}|} \sim |01\rangle$ con probabilidad $\langle\psi|P_{01}|\psi\rangle = |a_{01}|^2$

$\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|} = \frac{a_{10}|10\rangle}{|a_{10}|} \sim |10\rangle$ con probabilidad $\langle\psi|P_{10}|\psi\rangle = |a|^2_{10}$

$\frac{P_{ij}|\psi\rangle}{|P_{ij}|\psi\rangle|} = \frac{a_{11}|11\rangle}{|a_{11}|} \sim |11\rangle$ con probabilidad $\langle\psi|P_{11}|\psi\rangle = |a_{11}|^2$

Utilizando la medida del estado de dos cúbits se puede obtener información sobre la relación entre ellos, lo cual es de aplicación en los esquemas de corrección de errores. Sea V el espacio vectorial asociado con un sistema de dos cúbits y consideremos la medida asociada a la siguiente descomposición de suma directa: ciada $V = S_1 \oplus S_2$ donde S_1 es el subespacio generado por e $|00\rangle, |11\rangle$ es decir, el subespacio en el que los dos cúbits son iguales y S_2 es el subespacio generado por e $|01\rangle, |10\rangle$, el subespacio en el que los dos cúbits no son iguales. Sean P_1 y P_2 los proyectores correspondientes a S_1 y S_2 respectivamente. Cuando medimos un estado $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ de esta forma, el estado resultado será:

$\frac{P_i|\psi\rangle}{|P_i|\psi\rangle|}$ con probabilidad $\langle\psi|P_i|\psi\rangle = |P_i|\psi\rangle|^2$

Si definimos:

$c_1 = \langle\psi|P_1|\psi\rangle = \sqrt{|a_{00}|^2 + |a_{11}|^2}$ y

$c_2 = \langle\psi|P_2|\psi\rangle = \sqrt{|a_{01}|^2 + |a_{10}|^2}$

Tras la medición, el estado resultante será:

$|v\rangle = \frac{1}{c_1}(a_{00}|00\rangle + a_{11}|11\rangle$ con probabilidad $|c_1|^2 = |a_{00}|^2 + |a_{11}|^2$ y

$|v\rangle = \frac{1}{c_2}(a_{01}|01\rangle + a_{10}|10\rangle$ con probabilidad $|c_2|^2 = |a_{01}|^2 + |a_{10}|^2$

Si se observa el primer resultado, entonces, los dos cúbits son iguales aunque se desconoce si ambos son cuando $|0\rangle$ o ambos son $|1\rangle$. Por el contrario, si se observa el segundo resultado los cúbits son distintos aunque se desconoce cual de ellos tiene el estado $|0\rangle$ y cual el $|1\rangle$. La medida no proporciona el estado de los cúbits solo la relación entre ellos, iguales o distintos.

A continuación se muestra una medición en la que los subespacios asociados no están formados por subconjuntos de elementos de la base computacional o base estándar. Se realizará en esta ocasión una medida con respecto de la base de Bell. La base de Bell $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$, donde:

$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$

$|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle$

$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle$

$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle$

Sea V el espacio vectorial asociado con un sistema de dos cúbits y consideremos la medida asociada a la siguiente descomposición de suma directa de los subespacios generados por los estados de Bell: $V = S_{\Phi^+} \oplus S_{\Phi^-} \oplus S_{\Psi^+} \oplus S_{\Psi^+}$.

La medida del estado $|00\rangle$ con respecto a esta descomposición proporciona el estado $|\Phi^+\rangle$ con probabilidad $\frac{1}{2}$ y o $|\Phi^-\rangle$ con probabilidad $\frac{1}{2}$, ya que $|00\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle)$

La medida del estado $|11\rangle$ con respecto a esta descomposición proporciona el estado $|\Phi^+\rangle$ con probabilidad $\frac{1}{2}$ y o $|\Phi^-\rangle$ con probabilidad $\frac{1}{2}$, ya que $|11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle)$

La medida del estado $|01\rangle$ con respecto a esta descomposición proporciona el estado $|\Psi^+\rangle$ con probabilidad $\frac{1}{2}$ y o $|\Psi^-\rangle$ con probabilidad $\frac{1}{2}$, ya que $|01\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle)$

La medida del estado $|11\rangle$ con respecto a esta descomposición proporciona el estado $|\Psi^+\rangle$ con probabilidad $\frac{1}{2}$ y o $|\Psi^-\rangle$ con probabilidad $\frac{1}{2}$, ya que $|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle)$

Formalismo del operador hermítico para la medición

Ciertos operadores, llamados operadores hermíticos, definen una descomposición en subespacios ortogonales única, su descomposición en autoespacios. Además, para cada descomposición de este tipo, existe un operador hermítico cuya descomposición en autoespacios es esta descomposición. Dada esta correspondencia, los operadores hermíticos pueden usarse para describir mediciones.

Sea $O : V \to V$ un operador lineal. Si $O\vec{v} = \lambda\vec{v}$ para un vector distinto de cero $\vec{v} \in V$, entonces λ es un autovalor y $\vec{v}$ es su autovector asociado de O. Si tanto $\vec{v}$ como $\vec{w}$ son autovectores de O, entonces $\vec{v}+\vec{w}$ es también un autovector, por lo que el conjunto de todos los autovectores forma un subespacio de V llamado autoespacio de O. Para un operador con una representación de matriz diagonal, los autovalores son los valores a lo largo de la diagonal. Un operador $O : V \to V$ es hermítico si es igual a su adjunto,

$O^{\dagger} = O$.

Los autoespacios de los operadores hermíticos tienen propiedades especiales. Si λ es un autovalor de un operador hermíticos O con autovector $|x\rangle$entonces:

$\lambda\langle x|x\rangle = \langle x|\lambda|x\rangle = \langle x\lambda|(O|x\lambda\rangle) = (\langle x|O^{\dagger})|x\rangle = \bar{\lambda}\langle x|x\rangle$

$\lambda = \bar{\lambda}$

lo que significa que todos los autovalores de un operador hermítico son reales.

Para demostrar la relación entre los operadores hermíticos y las descomposiciones en subespacios ortogonales es necesario mostrar que los autoespacios $S_{\lambda 1}, S_{\lambda 2}, ..., S_{\lambda k}$ de un operador hermitico son ortogonales y satisfacen $S_{\lambda 1} \oplus S_{\lambda 2} \oplus \cdots \oplus S_{\lambda k} = V$.

Para cualquier operador, dos autovalores distintos tienen autoespacios disjuntos ya que para cualquier vector unitario $|x\rangle$, $O|x\rangle = \lambda_0|x\rangle$ y $O|x\rangle = \lambda_1|x\rangle$ lo que implica que

$(\lambda_0 - \lambda_1)|x\rangle = 0$ y por tanto $\lambda_0 = \lambda_1$

Para cualquier operador hermítico, los autovectores de autovalores distintos deben ser ortogonales.

Sea $|v\rangle$ un autovector asociado al autovalor λ y $|w\rangle$ otro autovector con autovalor μ distinto de λ. Entonces:

$\lambda\langle v|w\rangle = (\langle v|O^{\dagger})|w\rangle = \langle v|(O|w\rangle) = \mu\langle v|w\rangle$

Ya que λ y μ son autovalores distintos, $\langle v|w\rangle = 0$. Por lo tanto, S_{λ_i} y S_{λ_j} son ortogonales para $\lambda_i \neq \lambda_j$. La suma directa de todos los autoespacios de un operador hermítico $O : V \to V$ es el espacio V completo.

Sea V un espacio vectorial de dimensión N y sean $\lambda_1, \lambda_2, ..., \lambda_k$ con $k \leq N$ los autovalores distintos de un operador hermítico $O : V \to V$. Como se ha mostrado, $V = S_{\lambda_i} \oplus \cdots \oplus S_{\lambda_k}$, donde S_{λ_i} es el autoespacio de O con autovalor λ_i. Esta descomposición de suma directa de V se denomina descomposición en autoespacios de V para el operador hermítico O. Por lo tanto, cualquier operador hermítico $O : V \to V$ determina de manera única una descomposición en subespacios para V. Además, cualquier descomposición de un espacio vectorial V en la suma directa de los subespacios $S_1, ..., S_k$ se puede realizar como la descomposición en autoespacios de un operador hermítico $O : V \to V$: sean P_i los proyectores sobre los subespacios S_i, y sean $\lambda_1, \lambda_2, ..., \lambda_k$ cualquier conjunto de valores reales distintos, entonces, $O = \sum_{i=1}^{k} \lambda_i P_i$ es un operador hermítico con la descomposición de suma directa deseada.

Por todo lo anterior, al describir una medición, en lugar de especificar directamente la descomposición subespacial asociada, podemos especificar un operador hermítico cuya descomposición en autoespacios es esa descomposición.

Se puede utilizar cualquier operador hermítico con la descomposición de suma directa adecuada para especificar una medida determinada; en particular, los valores de λ_i son irrelevantes siempre que sean distintos. El λ_i debe considerarse simplemente como etiquetas para los subespacios correspondientes o, de manera equivalente, como etiquetas para los resultados de la medición. En física cuántica, estas etiquetas se eligen a menudo para representar una propiedad, como la energía, de los autoestados en el autoespacio correspondiente. En computación cuántica, no es necesario asignar etiquetas con significado, cualquier conjunto distinto de autovalores es igualmente válido.

Especificar una medición en términos de un operador hermítico es una práctica estándar en mecánica cuántica y computación cuántica, la medida no es el resultado de la acción del operador hermítico sobre el estado, los proyectores P_j asociados con un operador hermítico O, y no el propio O, son los que actúan sobre el estado. Qué proyector actúa sobre el estado depende de las probabilidades $p_j = \langle\psi|P_j|\psi\rangle$.

Por ejemplo, el resultado de medir $|\psi\rangle = a|0\rangle + b|1\rangle$ utilizando el operador hermítico $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$, no da como resultado el estado $a|0\rangle - b|1\rangle$, aunque:

$$Z\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} a \\ -b \end{pmatrix}$$

El operador hermítico es solo una forma de especificar la descomposición en subespacios asociada con la medida. La multiplicación directa de un operador hermítico por lo general no asegura producir, ni siquiera, un estado bien definido, como en el siguiente caso:

$$\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} |0\rangle = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

El postulado de la medición

Dado un estado desconocido de un cúbit $a|0\rangle + b|1\rangle$, no es posible experimentalmente conocer ese estado, el estado cuántico no es directamente observable. Solo podemos acceder a los resultados de las mediciones y por ello, los operadores hermíticos que utilizamos para realizar la medición, se denominan *observables*.

El postulado de medición de la mecánica cuántica establece que:

• Cualquier medida cuántica puede ser especificada por un operador hermítico O llamado observable.

• Los posibles resultados de medir un estado $|\psi\rangle$con un observable O corresponden con los autovalores de O. Así, la medición del estado $|\psi\rangle$ transforma el estado que corresponde al resultado correspondiente al autovalor λ_i de O con probabilidad $|P_i|\psi\rangle|^2$ siendo Pi el proyector en el autoespacio λ_i.

• (Proyección) El estado después de la medición es la proyección normalizada $\frac{Pi|\psi\rangle}{|Pi|\psi\rangle|}$ de $|\psi\rangle$ en el autoespacio S_i correspondiemte al autovalor λ_i. Por tanto, el estado después de la medición es un vector propio de longitud unitaria de O con autovalor λ_i.

Lo que se ha descrito es un formalismo matemático para la medición y no proporciona información sobre qué mediciones se pueden realizar experimentalmente. Algunas medidas que pueden ser matemáticamente simples pero muy difíciles de implementar. Además, los autovalores de las mediciones físicamente realizables pueden tener significado, como la posición o la energía de una partícula, pero los autovalores son simplemente etiquetas arbitrarias. Mientras que un operador hermítico especifica de forma única una descomposición en subespacios, para una descomposición dada hay muchos operadores hermíticos cuya descomposición en autoespacios es esa descomposición. En particular, dado que los autovalores son simplemente etiquetas para los subespacios o posibles resultados, los valores específicos de los autovalores son irrelevantes; sólo importa cuáles son distintos. Por ejemplo, midiendo con el operador hermítico $|0\rangle\langle 0| - |1\rangle\langle 1|$ resulta en los mismos estados con las mismas probabilidades que medir con $33|0\rangle\langle 0| - 33|1\rangle\langle 1|$, pero estos resultados no concuerdan con los resultados de la medición trivial correspondiente al operador hermítico $|0\rangle\langle 0|+|1\rangle\langle 1|$ o $42|0\rangle\langle 0| + 42|1\rangle\langle 1|$.

Supongamos un sistema de un cúbit para el que queremos construir un operador hermítico que especifique una medición en la base estándar. La descomposición en subespacios correspondiente a esta medida es $V = S \oplus S'$, donde S es el autoespacio generado por $|0\rangle$ y S' es el autoespacio generado por $|1\rangle$. Los proyectores asociados con S y S' son $P = |0\rangle\langle 0|$ y $P' = |1\rangle\langle 1|$ respectivamente. Tomemos dos valores reales cualquier $\lambda = 2$ and $\lambda' = -3$. entonces, el siguiente operador es un operador hermítico que especifica la medición de un estado de un cúbit en la base computacional:

$$O = 2|0\rangle\langle 0| - 3|1\rangle\langle 1| = \begin{pmatrix} 2 & 0 \\ 0 & -3 \end{pmatrix}$$

Se podrían haber tomado otros valores distintos para λ and λ'. En general se utilizarán los operadores $|1\rangle\langle 1| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ y $Z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ para especificar mediciones de un cúbit en la base computacional.

Para crear un operador hermítico que especifique la medida de un cúbit en la base de Hadamard $|+\rangle, |-\rangle$, tendremos que considerar la descomposición en los subespacios S_+, generado por$|+\rangle$, and S_-, generado por $|-\rangle$, con los proyectores asociados

$P_+ = |+\rangle\langle +| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$ y

$P_- = |-\rangle\langle -| = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|)$

Podemos escoger libremente λ_+ y λ_- siempre que sean distintos, si tomamos por ejemplo $\lambda_+ = 1$ y $\lambda = -1$ entonces el siguiente operador es un operador hermítico para la medición de un cúbit en la base de Hadamard:

$$X = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) - (\frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|)) = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

El siguiente operador, $O = 2|00\rangle\langle 00| + 7|01\rangle\langle 01| - 5|10\rangle\langle 10| + 3|11\rangle\langle 11|)$ es uno de los muchos operadores hermíticos que especifican una medida con respecto a una descomposición completa de la base computacional, la descomposición en autoespacios de O consiste en cuatro subespacios, cada uno generado por uno de los vectores de la base $|00\rangle, |01\rangle, |10\rangle, |11\rangle$.

$$O = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 7 & 0 & 0 \\ 0 & 0 & -5 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

El siguiente operador hermítico, $P = 2(|00\rangle\langle 00| + |01\rangle\langle 01|) + 9(|10\rangle\langle 10| + |11\rangle\langle 11|)$, especifica una medida para un sistema de dos cúbits con respecto a una descomposición en autoespacios, $V = S_0 \oplus S_1$ donde S_0 es generado por $|00\rangle, |01\rangle$ y S_1 es generado por $|10\rangle, |11\rangle$ de forma que P especifica una medida del primer cúbit en la base computacional.

$$P = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 9 & 0 \\ 0 & 0 & 0 & 9 \end{pmatrix}$$

El siguiente operador hermítico, $E = 5(|00\rangle\langle 00| + |11\rangle\langle 11|) + 6(|01\rangle\langle 01| + |10\rangle\langle 10|)$, especifica una medida para un sistema de dos cúbits con respecto a una descomposición en autoespacios, $V = S_0 \oplus S_1$ donde S_0 es generado por $|00\rangle, |11\rangle$ y S_1 es generado por $|01\rangle, |10\rangle$ de forma que E especifica una medida para comprobar si los cúbits tienen el mismo valor.

$$E = \begin{pmatrix} 5 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 5 \end{pmatrix}$$

Dada la descomposición subespacial para un operador hermítico O, es posible encontrar una base propia ortonormal de V para O. Si O tiene n autovalores distintos, como es el caso general, esa base es única excepto por un factor complejo de magnitud 1. Si O tiene menos de n autovalores, algunos de ellos están asociados con un autoespacio de más de una dimensión. En este caso, se puede elegir una base ortonormal aleatoria para cada autoespacio S_i. La matriz del operador hermítico O con respecto a cualquiera de estas bases propias es diagonal. Cualquier operador hermítico O, con autovalores λ_j, puede escribirse como $O = \sum_j \lambda_j P_j$, donde P_j son los proyectores correspondientes a los autovalores λ_j de O.

Todo proyector es hermítico con autovalores 1 y 0 donde el autoespacio correspondiente al autovalor 1 es la imagen del operador . Para un subespacio S de dimensión m de V generado por la base$|i_1\rangle, ..., |i_m\rangle$, el proyector asociado $P_S = \sum_j |i_j\rangle\langle i|$ asigna vectores en V a S.

Si P_S y P_T son proyectores para los subespacios ortogonales S y T, el proyector para la suma directa$S \oplus T$ es $P_S + P_T$. Si P es un proyector en el subespacio S, entonces $tr(P)$, la suma de los elementos diagonales de cualquier matriz que represente a P, es la dimensión de S. Este argumento se aplica a cualquier base ya que la traza es independiente de la base.

Dados los operadores lineales A y B en los espacios vectoriales V y W respectivamente, el producto tensor $A \otimes B$ actúa sobre los elementos $v \otimes w$ del espacio del producto tensorial $V \otimes W$ de la siguiente manera:

$(A \otimes B)(v \otimes w) = Av \otimes Bw$

De esta definición se deduce que $(A \otimes B)(C \otimes D) = AC \otimes BD$.

Sean O_0 y O_1 operadores hermíticos en los espacios V_0 y V_1 respectivamente. Entonces $O_0 \otimes O_1$ es un Operador hermítico en el espacio $V_0 \otimes V_1$. Además, si O_i tiene valores propios λ_{ij} con autoespacios asociados S_{ij}, entonces $O_0 \otimes O_1$ tiene autovalores $\lambda'_{jk} = \lambda_{0j}\lambda_{1k}$. Si un autovalor $\lambda'_{jk} = \lambda_{0j}\lambda_{1k}$ es único, entonces su autoespacio asociado S' es el producto tensorial de S_{0j} y S_{1k}. En general, los autovalores propios λ'_{jk} no necesitan ser distintos. Un valor propio λ' de $O_0 \otimes O_1$ que es el producto de utovalores de O_0 y O_1 de múltiples formas, $\lambda'_i = \lambda'_{j_1k_1} = \cdots = \lambda'_{j_mk_m}$, tiene el autoespacio $S = (S_{0j_1} \otimes S_{1k_1}) \oplus \cdots \oplus (S_{0j_m} \otimes S_{1k_m})$. La mayoría de los operadores hermíticos O en $V_0 \otimes V_1$ no se pueden escribir como un producto tensorial de dos operadores hermíticos O_0 y O_1 que actúan sobre V_0 y V_1 respectivamente. Tal descomposición es posible solo si cada subespacio en la descomposición de subespacios descrita por O puede escribirse como $S = S_0 \otimes S_1$ para S_0 y S_1 en las descomposiciones en subespacios asociadas con O_0 y O_1 respectivamente. Si bien para la mayoría de los operadores hermíticos esta condición no se cumple, sí se cumple para todos los observables que se han descrito anteriormente. Así, el siguiete producto tensorial especifica una medida completa en la base computacional

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix} = (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (2|0\rangle\langle 0| + 3|1\rangle\langle 1|)$$

o bien:

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -3 \end{pmatrix} = 2|00\rangle\langle 00| + 3|01\rangle\langle 01| - 2|10\rangle\langle 10| - 3|11\rangle\langle 11|$$

El operador siguiente especifica una medida del primer cúbit en la base computacional: $Z \otimes I$, donde: $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01|) - |10\rangle\langle 10| - |11\rangle\langle 11|$$

El operador : $Z \otimes Z = |00\rangle\langle 00| - |01\rangle\langle 01|) - |10\rangle\langle 10| + |11\rangle\langle 11|$, especifica una medida para determinar si los cúbits son iguales o no.

A continuación se muestra un ejemplo de una medida de dos cúbits que no puede ser expresada como un producto tensor de dos medidas de un cúbit, el observable con la siguiente matriz asociada:

$$K = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

determina si los dos bits tienen valor 1 o no. Las medidas realizadas con este operador dan como resultado un estado contenido en uno de dos subespacios S_0 y S_1, donde S_1 es el subespacio generado por $|11\rangle$ y S_0 el generado por $|00\rangle, |01\rangle, |10\rangle$. Medir con este operador es diferente a medir ambos cúbits en la base estándar y luego hacer *AND* de los resultados. Por ejemplo, el estado $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ no varía cuando se mide con K, pero la medida de ambos cúbits daría como resultado el estado $|01\rangle$ o $|10\rangle$ con igual probabilidad.

Se dice que un operador hermítico $Q_1 \otimes Q_2$ en un sistema de dos cúbit está compuesto por medidas de un cúbit si Q_1 y Q_2 son operadores hermíticos en los sistemas de un cúbit. Además, se dice que cualquier operador hermítico de la forma $Q \otimes I$ o $I \otimes Q'$ en un sistema de dos cúbit es una medida de un solo cúbit. De un modo más general, un operador hermítico de la forma $I \otimes \cdots \otimes I \otimes Q \otimes I \otimes \cdots \otimes I$ en un sistema de n cúbits se dice que es una medición de un solo cúbit del sistema. Cualquier operador hermítico de la forma $A \otimes I$ en un sistema $V \otimes W$, donde A es un operador hermítico que actúa sobre V, se dice que es una medida del subsistema V.

Como se ha explicado en secciones anteriores, solo se puede extraer un bit clásico de información de un bit cuántico, o cúbit. Se puede generalizar esta afirmación, dado que cualquier observable en un sistema de n cúbits tiene como máximo $2n$ autovalores distintos, hay como máximo $2n$ resultados posibles de una medición dada. Por lo tanto, una sola medición de un sistema de n cúbits revelará como máximo n bits de información clásica. Dado que, en general, la medición cambia el estado, cualquier medición adicional proporciona información sobre el nuevo estado, no sobre el original. En particular, si el observable tiene $2n$ autovalores distintos, la medición envía el estado a un autovector y por lo tanto cualquier medición adicional no podrá extraer ninguna información adicional sobre el estado original.

.

5.3 Referencias bibliográficas

Nielsen and Chuang (2011) Quantum Computation and Quantum Information

Aaronson (2013), Quantum Computing Since Democritus

Eric R. Johnston, Nic Harrigan y Mercedes Gimeno-Segovia (2019), Programming Quantum Computers

Eleanor Rieffel and Wolfgang Polak (2011), Quantum Computing

Robert Sutor (2019), Dancing with qubits