Computación Cuántica

Sistemas cuánticos de múltiples cúbits

Índice

Esquema

- Sistemas cuánticos de múltiples cúbits
  - Sistemas de mútiples cúbits
    - Espacio de estados exponencial
    - Producto tensor
  - Espacio de estados
    - Espacio de estados en un sistema de n cúbits
    - Estados entrelazados
  - Medida en sistemas de n cúbits
    - Dispositivo de medida
    - Descomposición del espacio vectorial
    - Bases
  - Distribución cuántica de clave con entrelazamiento

Ideas clave

4.1 Introducción y objetivos

A diferencia de los sistemas clásicos, el espacio de estados de un sistema cuántico crece exponencialmente con el número de partículas. Por lo tanto, cuando codificamos información en estados cuánticos de un sistema de n partículas, hay muchos más estados disponibles que cuando se usan estados clásicos para codificar la información. Esta extraordinaria propiedad de generar enormes espacios de estados con un número de componentes físicos mucho menor y como ello puede aprovecharse para acelerar la computación es el tema principal del resto de esta asignatura.

> *Por cada cúbit que añadimos al sistema, la dimensión del espacio vectorial se duplica, este crecimiento es, por tanto, exponencial.*

La enorme diferencia en la dimensión entre los espacios de estados clásico y cuántico se debe a una diferencia en la forma en que se combinan los espacios. En un sistema físico clásico, macroscópico, que consta de varios componentes, el estado del sistema se puede caracterizar completamente describiendo el estado de cada una de sus componentes por separado. Un aspecto sorprendente y poco intuitivo de los sistemas cuánticos es que, en general, el estado de un sistema no puede describirse en términos de los estados de sus componentes y los estados que no pueden describirse así se denominan estados entrelazados. El entrelazamiento es una herramienta fundamental de la computación cuántica. La siguiente figura muestra una representación con círculos de dos cúbits entrelazados, solo los estados en los que ambos cúbits tienen el mismo valor están permitidos.

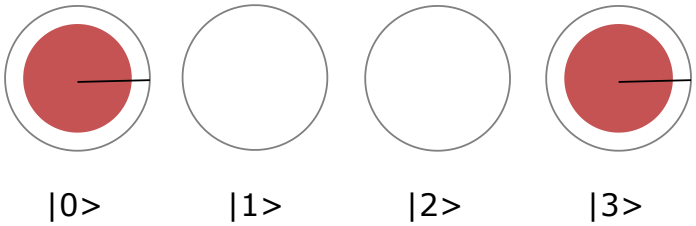

Figura 1: Dos cúbits entrelazados utilizando la representación con círculos. Elaboración propia.

Los estados entrelazados son un fenómeno exclusivamente cuántico, no existe un comportamiento semejante en la física clásica. La mayoría de los estados en un sistema de múltiples cúbits son estados entrelazados, son lo que llena los vastos espacios de estados cuánticos.

La imposibilidad de simular eficientemente el comportamiento de los estados entrelazados utilizando computadoras clásicas fue la base para que los pioneros de este campo consideraran la posibilidad de usar este comportamiento para computar con mayor eficiencia, lo que condujo al nacimiento y desarrollo del campo de la computación cuántica.

En este tema estudiaremos el espacio de estados de sistemas compuestos de múltiples cúbits y como el producto tensor permite combinar los espacios vectoriales de ellos. A continuación se tratarán los estados entrelazados, que proporcionan una herramientas fundamental de la computación cuántica. Finalmente se extenderán los conceptos tratados en temas anteriores sobre la medida de un cúbit a sistemas de múltiples cúbits y una aplicación del entrelazamiento, la distribución de clave cuántica aprovechando esta propiedad.

- Los sistemas cuánticos de múltiples cúbits
- El espacio de estados cuántico
- El producto tensor
- El espacio de estados de un sistema cuántico de n cúbits
- Estados entrelazados

- La medida en los sistemas de múltiples cúbits
- Distribución cuántica de clave con entrelazamiento

4.2 Un espacio de estados exponencial

En la física clásica, los posibles estados de un sistema formado por n objetos, cuyos estados individuales pueden ser descritos por un vector en un espacio vectorial bidimensional, pueden modelarse en un espacio vectorial de $2n$ dimensiones. Los espacios de estado clásicos se combinan a través de la suma directa. Sin embargo, el espacio de estados combinado de n sistemas cuánticos, cada uno con estados descritos por vectores bidimensionales, es mucho mayor. Los espacios vectoriales asociados con los sistemas cuánticos se combinan a través del producto tensorial, lo que da como resultado un espacio vectorial de 2^n dimensiones. Veamos la definición formal de la suma directa así como del producto tensorial para compararlos y la diferencia de tamaño entre los espacios resultantes.

La suma directa $V \oplus W$ de dos espacios vectoriales V y W, con bases:

$$A = |\alpha_1\rangle, |\alpha_2\rangle, ..., |\alpha_n\rangle$$

$$B = |\beta_1\rangle, |\beta_2\rangle, ..., |\beta_m\rangle$$

respectivamente, es el espacio vectorial con base:

$$A \bigcup B = |\alpha_1\rangle, |\alpha_2\rangle, ..., |\alpha_n\rangle, |\beta_1\rangle, |\beta_2\rangle, ..., |\beta_m\rangle.$$

El orden de la base es arbitrario. Cada elemento $|x\rangle \in V \oplus W$ puede escribirse como $|x\rangle = |v\rangle \oplus |w\rangle$ para algunos $|v\rangle \in V$ y$|w\rangle \in W$. Donde la dimensión de V y W es n y m respectivamente, $V \oplus W$ tiene dimensión $n + m$:

$$dim(V \oplus W) = dim(V) + dim(W).$$

La suma y la multiplicación escalar se definen realizando la operación en los espacios vectoriales de dos componentes por separado y sumando los resultados. Cuando V y

W son espacios con producto interno, el producto interno estándar en $V \oplus W$ viene dado por:

$$(\langle v_2| \oplus \langle w_2|)(|v_1\rangle \oplus |w_1\rangle) = \langle v_2|v_1\rangle + \langle w_2|w_1\rangle.$$

El espacio de estados de n objetos clásicos tiene dimensión 2n. Por tanto, el tamaño del espacio de estados crece linealmente con el número de objetos. Así, si el estado de cada uno de tres objetos clásicos O_1, O_2 y O_3 está completamente descrito por dos parámetros, la posición x_i y la cantidad de movimiento p_i, entonces, el estado del sistema se puede describir mediante la suma directa de los estados de los objetos individuales:

$$\begin{pmatrix} x_1 \\ p_1 \end{pmatrix} \oplus \begin{pmatrix} x_2 \\ p_2 \end{pmatrix} \oplus \begin{pmatrix} x_3 \\ p_3 \end{pmatrix} = \begin{pmatrix} x_1 \\ p_1 \\ x_2 \\ p_2 \\ x_3 \\ p_3 \end{pmatrix}$$

4.3 El producto tensor

El producto tensorial, que representamos como: $V \otimes W$, de dos espacios vectoriales V y W con bases $A = |\alpha_1\rangle, |\alpha_2\rangle, ..., |\alpha_n\rangle$ y $B = |\beta_1\rangle, |\beta_2\rangle, ..., |\beta_m\rangle$respectivamente es un espacio vectorial de dimensión nm con una base que consta de los elementos nm de la forma $|\alpha_i\rangle \otimes |\beta_j\rangle$ donde $\otimes$ es el producto tensorial, un operador binario abstracto que satisface las siguientes relaciones:

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle$$

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle$$

$$(a|v\rangle) \otimes |w\rangle = |v\rangle \otimes (a|w\rangle) = a(|v\rangle \otimes |w\rangle).$$

Tomando $k = min(n, m)$, todos los elementos de $V \otimes W$ tienen forma: $|v_1\rangle \otimes |w_1\rangle +$

$|v_2\rangle \otimes |w_2\rangle + \cdots + |v_k\rangle \otimes |w_k\rangle$, donde $v_i \in V$ y $w_i \in W$. Debido a las relaciones que definen el producto tensorial, dicha representación no es única. Además, aunque todos los elementos de $V \otimes W$ se pueden escribir de la forma $\alpha_1(|\alpha_1\rangle \otimes |\beta_1\rangle) + \alpha_2(|\alpha_2\rangle \otimes |\beta_1\rangle) + \cdots + \alpha_{nm}(|\alpha_n\rangle \otimes |\beta_m\rangle)$, la mayoría de los elementos de $V \otimes W$ no se pueden escribir como $|v\rangle \otimes |w\rangle$, donde $v \in V$ y $w \in W$.

Un elemento como $|v\rangle \otimes |w\rangle$ suele expresarse de forma más compacta como $|v\rangle|w\rangle$ o incluso $|vw\rangle$.

Si V y W son espacios con producto interno, entonces a $V \otimes W$ puede tener un producto interno a partir del producto de los productos internos en V y W; el producto interno de $|v_1\rangle \otimes |w_1\rangle$ y $|v_2\rangle \otimes |w_2\rangle$ viene dado por:

$$(\langle v_2| \otimes \langle w_2|) \cdot (|v_1\rangle \otimes |w_1\rangle) = \langle v_2|v_1\rangle\langle w_2|w_1\rangle,$$

El producto tensorial de dos vectores unitarios es un vector unitario, y dadas las bases ortonormales $|\alpha_i\rangle$ para V y$|\beta_i\rangle$ para W, la base $|\alpha_i\rangle \otimes |\beta_j\rangle$, para $V \otimes W$, también es ortonormal . El producto tensorial $V \otimes W$ tiene dimensión $dim(V) \times dim(W)$, por lo que el producto tensorial de n espacios vectoriales bidimensionales tiene 2^n dimensiones. La mayoría de los elementos $|w\rangle \in V \otimes W$ no se pueden escribir como el producto tensorial de un vector en V y un vector en W (aunque todos son combinaciones lineales de dichos elementos). Esta observación es de crucial importancia para la computación cuántica. Los estados de $V \otimes W$ que no pueden escribirse como el producto tensorial de un vector en V y un vector en W se denominan estados entrelazados. Como veremos, para la mayoría de los estados cuánticos de un sistema de n-cúbit, en particular para todos los estados entrelazados, no tiene sentido hablar del estado de un cúbit del sistema.

4.4 El espacio de estado de un sistema de n cúbits

Dados dos sistemas cuánticos con estados representados por vectores unitarios en V y W respectivamente, los posibles estados del sistema cuántico conjunto están representados por vectores unitarios en el espacio vectorial $V \otimes W$. Para $0 \leq i < n$, sea V_i el espacio vectorial, con base $|0\rangle_i$, $|1\rangle_i$, correspondiente a un cúbit, entonces, la base estándar para el espacio vectorial $V_{n-1} \otimes \cdots \otimes V_1 \otimes V_0$ para el sistema de n cúbits está formada por 2^n vectores.

$\{|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |0\rangle_0,$

$|0\rangle_{n-1} \otimes \cdots \otimes |0\rangle_1 \otimes |1\rangle_0,$

$|0\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |0\rangle_0,$

...

$|1\rangle_{n-1} \otimes \cdots \otimes |1\rangle_1 \otimes |1\rangle_0\}$

A menudo se omiten los subíndices ya que el correspondiente cúbit se ceduce de su posición. La convención de que los kets adayacentes representan su producto tensorial, podemos reescribr la base de una forma más compacta:

$\{|0\rangle \cdots |0\rangle|0\rangle,$

$|0\rangle \cdots |0\rangle|1\rangle,$

$|0\rangle \cdots |1\rangle|0\rangle,$

...

$|1\rangle \cdots |1\rangle|1\rangle\}$

Y dado que el espacio correspondiente al producto tensorial de un sistema de n cúbits es tan frecuente se usa una notación todavía más compacta:

$|b_{n-1}...b_0\rangle$ para representar $|b_{n-1}\rangle \otimes \cdots \otimes |b_0\rangle$.

En esta notación se puede escribir la base estándar para un sistema de n cúbits como:

$|0\cdots00\rangle, |0\cdots01\rangle, |0\cdots10\rangle, \ldots, |1\cdots11\rangle.$

Finalmente, dado que la notación decimal es más compacta que la notación binaria, representaremos el estado $|b_{n-1}\ldots b_0\rangle$ como $|x\rangle$, donde b_i son los dígitos de la representación binaria del número decimal x. De esta forma, en esta notación, la base estándar para un sistema de 3 cúbits sería:

$\{|0\rangle_2 \otimes |0\rangle_1 \otimes |0\rangle_0,$

$|0\rangle_2 \otimes |0\rangle_1 \otimes |1\rangle_0,$

$|0\rangle_2 \otimes |1\rangle \otimes |0\rangle_0,$

$|0\rangle_2 \otimes |1\rangle \otimes |1\rangle_0,$

$|1\rangle_2 \otimes |0\rangle_1 \otimes |0\rangle_0,$

$|1\rangle_2 \otimes |0\rangle_1 \otimes |1\rangle_0,$

$|1\rangle_2 \otimes |1\rangle \otimes |0\rangle_0,$

$|1\rangle_2 \otimes |1\rangle \otimes |1\rangle_0\}$

o bien:

$\{|0\rangle|0\rangle|0\rangle, |0\rangle|0\rangle|1\rangle,|0\rangle|1\rangle|0\rangle,|0\rangle|1\rangle|1\rangle,|1\rangle|0\rangle|0\rangle, |1\rangle|0\rangle|1\rangle,|1\rangle|1\rangle|0\rangle,|1\rangle|1\rangle|1\rangle\}$

o de forma más compacta:

$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle = |0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle.$

En general, para un sistema de n cúbits se escribe:

$|0\rangle, |1\rangle, |2\rangle, \ldots, |2^n - 1\rangle.$

Por tanto, la base estándar para un sistema de dos cúbits se puede escribir como:

$|0\rangle, |1\rangle, |2\rangle, |3\rangle,$

y la base estándar para un sistema de tres cúbit se puede escribir como:

$|0\rangle, |1\rangle, |2\rangle, |3\rangle, |4\rangle, |5\rangle, |6\rangle, |7\rangle$.

Dado que la notación $|3\rangle$,por ejemplo, corresponde a dos estados diferentes en estas dos bases, uno es un estado de dos cúbits y el otro un estado de tres cúbits, para que dicha notación sea inequívoca, el número de cúbits debe quedar claro a partir del contexto.

Para utilizar la notación matricial para los vectores de estado de un sistema de n cúbits, se debe establecer el orden de los vectores base y, a menos que se especifique lo contrario, se supone que los vectores base están ordenados numéricamente. Usando esta convención, el estado de dos cúbit $\frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{2}|0\rangle + \frac{i}{2}|1\rangle + \frac{1}{\sqrt{2}}|3\rangle$ tendrá la siguiente representación matricial:

$$\begin{pmatrix} \frac{1}{2} \\ \frac{i}{2} \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix}$$

Normalmente utilizaremos la base estándar o base computacional, sin embargo, usaremos también otras bases, como la base de Bell para un sistema de dos cúbits. La base de Bell es una base de importancia fundamental en computación cuántica, utilizada en aplicaciones como la teleportación cuántica. La base de Bell esta formada por los siguientes estados:

$|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$, donde:

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

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

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

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

Como en el caso de un solo cúbit, un estado $|v\rangle$ es una superposición con respecto a un conjunto de estados ortonormales $|\beta_1\rangle, |\beta_2\rangle, ..., |\beta_i\rangle$, si es una combinación lineal de estos estados, $|v\rangle = a_1|\beta_1\rangle + a_2|\beta_2\rangle + ... + a_i|\beta_i\rangle$, y al menos dos de los coeficientes a_i son distintos de cero. Si no se especifica un conjunto de estados ortonormales, se

supondrá que la superposición es con respecto a la base estándar o base computacional.

Cualquier vector unitario del espacio de estados de dimensión 2^n representa un estado válido de un sistema de n-cúbit, pero, al igual que en el caso de un solo cúbit, hay redundancia. En el caso de múltiples cúbits, no solo los vectores que son múltiplos entre sí hacen referencia al mismo estado, sino que las propiedades del producto tensorial también significan que los factores de fase se distribuyen entre los productos tensoriales; la misma fase, en diferentes cúbits de un producto tensorial, representa el mismo estado:

$$|v\rangle \otimes (e^{i\varphi}|w\rangle) = e^{i\varphi}(|v\rangle \otimes |w\rangle) = (e^{i\varphi}|v\rangle) \otimes |w\rangle$$

Como en el caso de un solo cúbit, los vectores que tan solo se diferencian en la fase global, representan el misma estado cuántico. Los factores de fase en cúbits individuales de un solo término de una superposición siempre se pueden factorizar en un solo coeficiente para ese término.

Si representamos cada estado cuantico como:

$$a_0|0...00\rangle + a_2|0...01\rangle + ... + a_{2^n-1}|1...11\rangle$$

y el primer coeficiente a_i distinto de zero es real y no es negativo, entonces, cada estado cuántico tiene una representación única. Dado que esta representación representa de forma única estados cuánticos, el espacio de estados cuánticos de un sistema de n-cúbit tiene $2^n - 1$ dimensiones complejas. Para cualquier espacio vectorial complejo de dimensión N, el espacio en el que los vectores que son múltiplos entre sí se consideran equivalentes se denomina espacio proyectivo complejo de dimensión N - 1. Por tanto, el espacio de estados cuánticos distintos de un sistema de n-cúbit es un spacio proyectivo complejo de dimensión $2^n - 1$. Al igual que en el caso de un solo cúbit, debemos tener cuidado de no confundir el espacio vectorial en el que escribimos nuestros cálculos con el propio espacio de estados cuánticos. Nuevamente, debemos tener cuidado de evitar confusión entre las fases relativas entre términos en la superposición, de importancia crítica en mecánica cuántica, y la fase global que no tiene significado físico. Escribimos $|v\rangle \sim |w\rangle$ para indicar que los dos vectores $|v\rangle$ y $|w\rangle$ difieren solo

en una fase global y por lo tanto representan el mismo estado cuántico. Por ejemplo, aunque $|00\rangle \sim e^{i\varphi}|00\rangle$, los vectores $|v\rangle = \frac{1}{\sqrt{2}}(e^{i\varphi}|00\rangle + |11\rangle)$ y $|w\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ representan diferentes estados cuánticos, que se comportan de manera diferente en muchas situaciones:

$$\frac{1}{\sqrt{2}}(e^{i\varphi}|00\rangle + |11\rangle)] \sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Sin embargo:

$$\frac{1}{\sqrt{2}}(e^{i\varphi}|00\rangle + e^{i\varphi}|11\rangle) \sim \frac{e^{i\varphi}}{\sqrt{2}}(|00\rangle + |11\rangle) \sim \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Los cálculos en mecánica cuántica generalmente se realizan en el espacio vectorial en lugar de en el espacio proyectivo porque la linealidad facilita el trabajo con los espacios vectoriales. Pero siempre debemos tener en cuenta la equivalencia entre estados que solo difieren en una fase global cuando interpretamos los resultados.

La confusión también surge al utilizar diferentes bases, por ejemplo, usando la base de Hadamard, donde:

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

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

La expresión:

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

es una forma diferente de escribir $|0\rangle$y

$$\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \text{ y } \frac{1}{\sqrt{2}}(|+\rangle|+\rangle + |-\rangle|-\rangle)$$

son expresiones del mismo vector.

4.5 Estados entrelazados

Como vimos, el estado de un cúbit puede especificarse mediante un solo número complejo, por lo que cualquier producto tensorial de n estados individuales de un solo cúbit se puede especificar mediante n números complejos. Sin embargo necesitamos $2^n - 1$ números complejos para describir el estado de un sistema de n cúbits. Puesto que 2^n es un número muy superior a n, la enorme mayoría de estados de n cúbits no se pueden describir en términos del estado de n sistemas separados de un solo cúbit. Los estados que no pueden escribirse como el producto tensorial de n estados de un solo cúbit se denominan estados entrelazados y por tanto, la gran mayoría de los estados cuánticos están entrelazados.

Los estados que forman la base de Bell son un ejemplo de estados entrelazados. Así, el estado $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ no puede describirse en términos del estado de cada uno de sus dos cúbits por separado. Este estado no se puede descomponer, ya que no existen unos a_1, a_2, b_1, b_2 tal que:

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

puesto que:

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$$

y por tanto: $a_1b_2 = 0$

luego: $a_1a_2 = 0$ o bien: $b_1b_2 = 0$

Los distintos estados de Bell son otros ejemplos de estados entrelazados, como lo son también los siguientes estados:

$\frac{7}{10}|00\rangle + \frac{\sqrt{51}}{10}|11\rangle$,

$\frac{3}{10}|00\rangle + \frac{4}{10}|01\rangle + \frac{\sqrt{24}}{10}|11\rangle + \frac{\sqrt{51}}{10}|11\rangle$,

$\frac{1}{\sqrt{2}}(|01\rangle + i|10\rangle)$

Estrictamente hablando, el entrelazamiento es siempre con respecto a una descomposición específica en producto tensorial del espacio de estados. Es decir, dado un estado

$|\psi\rangle$ de un sistema cuántico con espacio vectorial asociado V y una descomposición tensorial de V, $V = V_1 \otimes \cdots \otimes V_n$, el estado $|\psi\rangle$ es *separable*, o no entrelazado, con respecto a esa descomposición si se puede expresar $|\psi\rangle$ como: $|\psi\rangle = |v_1\rangle \otimes \cdots \otimes |v_n\rangle$, donde $|v_i\rangle$ está contenido en V_i. De lo contrario, $|\psi\rangle$ se considera entrelazado con respecto de esa descomposición. A menos que se especifique una descomposición diferente, que un estado de n-cúbit está entrelazado, significa que está entrelazado con respecto a la descomposición del producto tensorial del espacio vectorial V asociado al sistema de n cúbits en los n espacios vectoriales bidimensionales $V_{n-1}, \ldots V_0$ asociados con cada uno de los cúbits individuales. Deberá especificarse, o dejar claro a partir del contexto, cuál de las muchas descomposiciones posibles de V en espacios de dos dimensiones corresponde con el conjunto de cúbits en consideración.

El entrelazamiento no es una propiedad absoluta de un estado cuántico, sino que depende de la descomposición particular del sistema en subsistemas considerados; estados entrelazados con respecto a la descomposición de un solo cúbit pueden no estar entrelazados con respecto a otras descomposiciones en subsistemas. En particular, al tratar el entrelazamiento en la computación cuántica, nos interesará el entrelazamiento con respecto a una descomposición en registros cuánticos, subsistemas que constan de múltiples cúbits, así como el entrelazamiento con respecto a la descomposición en cúbits individuales.

El siguiente ejemplo demuestra cómo un estado puede estar entrelazado con respecto a una descomposición y no con respecto a otra. El estado de cuatro cúbits siguiente está entrelazado porque no podemos expresarlo como un producto tensor de los cuatro estados correspondientes a los estados de cada cúbit individual. Este entrelazamiento es con respecto a la descomposición en cúbits y queda claro en el contexto.

$$|\psi\rangle = \frac{1}{2}(|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle)$$

Pero con respecto a otra descomposición este estado no está entrelazado, por ejemplo sería posible expresar el estado como:

$$|\psi\rangle = \frac{1}{2}(|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4 + |0\rangle_1|1\rangle_2|0\rangle_3|1\rangle_4 + |1\rangle_1|0\rangle_2|1\rangle_1|0\rangle_4 + |1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4) = \frac{1}{\sqrt{2}}(|0\rangle_1|0\rangle_3 + |1\rangle_1|1\rangle_3) \otimes \frac{1}{\sqrt{2}}(|0\rangle_2|0\rangle_4 + |1\rangle_2|1\rangle_4)$$

El estado no esta entrelazado con respecto a un descomposici´pon del sistema que consiste en un subsistema formado por los cúbits primero y tercero y otro subsistema formado por los cúbits segundo y cuarto. Sin embargo, también estaría entrelazado con respecto a la descomposición en dos subsistemas formados por dos cúbits cada uno: primero y segundo, tercero y cuarto.

El concepto de entrelazamiento no depende de la base, aunque depende de la descomposición, no hay ninguna dependencia de la base en la definición de entrelazamiento. Ciertas bases pueden ser más o menos convenientes para trabajar con un entrelazamiento al reflejar mejor o peor la descomposición en consideración, pero la elección de la base no afecta al entrelazamiento

Como en el caso de un solo cúbit, la mayoría de los estados de un sistema formado por n cúbits son superposiciones, combinaciones lineales no triviales de vectores básicos. Como siempre, la noción de superposición depende de la base; todos los estados son superposiciones con respecto a algunas bases, y no lo son con respecto a otras bases. Para múltiples cúbits, el significado de la superposición es más complicada que en el caso de un solo cúbit. La forma común de hablar sobre la superposición diciendo que el sistema está en dos estados *al mismo tiempo* es todavia más inapropiada para el caso de múltiples cúbits. Por ejemplo, no permitiría distinguir entre estados como $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ y $\frac{1}{\sqrt{2}}(|00\rangle + i|11\rangle)$ que tan solo se diferencian por su fase relativa pero que se comportan de manera diferente. Además, el concepto de estar *estar al mismo tiempo* es dependiente de la base, las expresiones:

$$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

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

representan el mismo estado pero tendrían diferentes interpretaciones, una como si estuviera en los estados $|00\rangle$ y $|11\rangle$ al mismo tiempo, y la otra como si estuviera en los estados $|++\rangle$ y $|--\rangle$ al mismo tiempo, a pesar de ser el mismo estado y, por lo tanto, comportarse exactamente de la misma forma en todas las circunstancias.

El ejemplo anterior refuerza el hecho de que las superposiciones cuánticas no son mezclas probabilísticas. No obstante, y siempre que no se interprete de forma literal,

la idea de pensar en las superposiciones como si el sistema estuviera en múltiples estados a la vez puede ser útil al principio para facilitar el entendimiento.

El entrelazamiento entre cúbits no solo es fundamental para entender el tamaño exponencial de los espacios de estados cuánticos de los sistemas de múltiples cúbits, las partículas en un estado entrelazado también pueden aprovecharse para la comunicación de información tanto clásica como cuántica y además, los algoritmos cuánticos aprovechan el entrelazamiento para acelerar el procesamiento de la información. La forma en la que se comportan los estados entrelazados frente a la medida es uno de los temas centrales de la mecánica cuántica, así como una herramienta fundamental en el procesamiento cuántico de la información.

Utilizando el entorno de desarrollo de QISKit Quantum Lab, realiza el siguiente experimento que muestra la visualización del estado y el circuito.

Ejemplo 1. Creación de un circuito de un cúbit e inicialización del estado

```
# Importar las librerias de QISKit necesarias

from qiskit import QuantumCircuit

from qiskit_textbook.tools import array_to_latex

# Crear un circuito cuántico de un cúbit

qc = QuantumCircuit(1)

# Definir el estado inicial a |1>

ket = [0,1]

# Visualizar el ket

array_to_latex(ket, pretext = "\\text{|1>} = ", precision=1)

# Aplicar la operación de inicialización al cúbit

qc.initialize(ket, 0)
```

```
# Dibujar el circuito

qc.draw()
```

Utilizando el entorno de desarrollo de QISKit Quantum Lab, realiza el siguiente experimento que muestra la visualización de un estado entrelazado.

Ejemplo 2. Creación de un circuito de tres cúbits e inicialización del estado entrelazado $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$

```
# Importar las librerias de QISKit necesarias

from qiskit import QuantumCircuit

from qiskit_textbook.tools import array_to_latex

import numpy as np

# Crear un circuito cuántico de dos cúbits

qc = QuantumCircuit(3)

# Definir el estado inicial

ket = [1,0,0,0,0,0,0,1]/np.sqrt(2)

# Visualizar el ket

array_to_latex(ket, pretext = "\\text{|1>} = ", precision=1)

# Aplicar la operación de inicialización a los cúbits

qc.initialize(ket,[0,1,2])

# Dibujar el circuito

qc.draw()
```

4.6 La medida en los sistemas de múltiples cúbits

Los experimentos con fotones que se describieron anteriormente muestran como la medida de un cúbit es probabilística y transforma el estado cuántico en un estado compatible con el dispositivo de medida. Cuando el sistema está formado por múltiples cúbits ocurre lo mismo con la salvedad de que el conjunto de medidas posibles así como de los resultados de las medidas es significativamente más rico que en el caso de un unico cúbit.

Supongamos un sistema formado por n cúbits siendo $N = 2^n$ la dimensión del espacio vectorial V asociado a él. Cualquier dispositivo que mida este sistema tiene una descomposición como suma directa asociada en subespacios ortogonales:$V = S_1 \oplus \cdots \oplus S_k$donde $k \leqslant N$corresponde al número máximo de posibles resultados de un estado medido con ese dispositivo en particular. Este número varía para diferentes dispositivos, incluso en dispositivos que miden el mismo sistema. El hecho de que cada dispositivo tenga una descomposición como suma directa asociada es una generalización del caso de un sistema formado por un único cúbit. Cada dispositivo que mide el estado de un sistema formado por un cúbit tiene una base ortonormal asociada $|\beta_1\rangle, |\beta_2\rangle$ para el espacio vectorial V asociado al sistema de un cúbit. Cada uno de los vectores $|\beta_i\rangle$genera un subespacio S_i formado por todos los $a|\beta_i\rangle$ donde a es un número complejo y $V = S1 \oplus S2$. Además, las únicas descomposiciones no triviales del espacio vectorial V son en dos subespacios unidimensionales, y cualquier elección de vectores de longitud unitaria, uno de cada uno de los subespacios, produce una base ortonormal.

Cuando un dispositivo de medición con descomposición de suma directa asociada $V = S_1 \oplus \cdots \oplus S_k$ interactúa con un sistema de n cúbits que se encuentra en el estado $|\psi\rangle$, la interacción modifica el estado a uno completamente contenido dentro de uno de los subespacios, y elige el subespacio con probabilidad igual al cuadrado del valor absoluto de la amplitud del componente de $|\psi\rangle$ en ese subespacio. Más formalmente, el estado $|\psi\rangle$ tiene una descomposición de suma directa única $|\psi\rangle = a_1|\psi_1\rangle \oplus \cdots \oplus$

$a_k|\psi_k\rangle$, donde $|\psi_i\rangle$ es un vector unitario en S_i y el coeficiente a_i es real y no negativo. Al medir el estado $|\psi\rangle$ se obtiene el estado $|\psi_i\rangle$ con probabilidad $|a_i|^2$. Que cualquier dispositivo de medición tenga asociada una descomposición de suma directa, y que la interacción pueda modelarse de esta manera, es un axioma de la mecánica cuántica, no es posible demostrar que todos los dispositivos se comportan de esta manera, pero hasta ahora ha proporcionado un modelo excelente que predice el resultado de los experimentos con gran precisión.

La medida del estado de un sistema cuántico formado por un solo cúbit en la base estándar sería de la siguiente forma: sea V el espacio vectorial asociado al sistema de un solo cúbit. Un dispositivo de medida de un cúbit en la base estándar tiene, por definición, la siguiente descomposición de suma directa asociada $V = S_1 \oplus S_2$, donde S_1 es generado por $|0\rangle$ y S_2 es generado por $|1\rangle$. Un estado arbitrario $|\psi\rangle = a|0\rangle + b|1\rangle$ medido por tal dispositivo proporcionará el estado $|0\rangle$ con probabilidad $|a|^2$, con a, la amplitud de $|\psi\rangle$ en el subespacio S_1, y $|1\rangle$ con probabilidad $|b|^2$, con b, la amplitud de $|\psi\rangle$ en el subespacio S_1. Un dispositivo que mida ese mismo sistema en la base de Hadamard:

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

tiene una descomposición en subespacios asociada $V = S_+ \oplus S_-$, donde S_+ es generado por $|+\rangle$ y $S_$es generado por $|-\rangle$.

Un estado $|\psi\rangle = a|0\rangle + b|1\rangle$ se puede reescribir como:

$$|\psi\rangle = \frac{a+b}{\sqrt{2}}|+\rangle + \frac{a-b}{\sqrt{2}}|-\rangle,$$

y por tanto, la probabilidad de que $|\psi\rangle$ se mida como $|+\rangle$ será $|\frac{a+b}{\sqrt{2}}|^2$ y la probabilidad de que el resultado de la medida sea $|-\rangle$ será $|\frac{a-b}{\sqrt{2}}|^2$.

La medida del estado del primer cúbit de un sistema cuántico formado por dos cúbits en la base estándar sería de la siguiente forma: sea V el espacio vectorial asociado al sistema de dos cúbits. Un dispositivo de medida que mida el primero de los dos cúbits en la base estándar tiene, por definición, la descomposición de suma directa asociada $V = S_1 \oplus S_2$, donde $S_1 = |0\rangle \otimes V_2$, es decir, el subespacio de dos dimensiones generado por $|00\rangle, |01\rangle$ y $S_2 = |1\rangle \otimes V_2$ el generado por $|10\rangle, |11\rangle$.

Un estado arbitrario $|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$ que podemos escribir como:

$$|\psi\rangle = c_1|\psi_1\rangle + c_2|\psi_2\rangle$$

donde:

$|\psi_1\rangle = \frac{1}{c_1}(a_{00}|00\rangle + a_{01}|01\rangle) \in S_1$ y

$|\psi_2\rangle = \frac{1}{c_2}(a_{10}|10\rangle + a_{11}|11\rangle) \in S_2$

siendo:

$c_1 = \sqrt{|a_{00}|^2 + |a_{01}|^2}$ y

$c_2 = \sqrt{|a_{10}|^2 + |a_{11}|^2}$

los factores de normalización.

Una medida del estado $|\psi\rangle$ realizada por ese dispositivo proporcionará el estado $|\psi_1\rangle$ con probabilidad $|c_1|^2 = |a_{00}|^2 + |a_{01}|^2$, y el estado $|\psi_2\rangle$ con probabilidad $|c_2|^2 = |a_{10}|^2 + |a_{11}|^2$.

En el caso especial del estado de Bell $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ la medida proporcionará uno de los dos estados $|00\rangle$ y $|11\rangle$con la misma probabilidad $\frac{1}{2}$.

La medida del primer cúbit de ese mismo sistema formado por dos cúbits, utilizando un dispositivo que mida con respecto a la base de Hadamard:

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

tiene una descomposición en subespacios asociada $V = S'_1 \oplus S'_2$, donde $S'_1 = |+\rangle \otimes V_2$ es el subespacio de dos dimensiones generado por:

$|+\rangle|0\rangle, |+\rangle|1\rangle$ y $S'_2 = |-\rangle \otimes V_2$.

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

$$|\psi\rangle = a'_1|\psi'_1\rangle + a'_2|\psi'_2\rangle$$

donde:

$|\psi_1'\rangle = c_1'(\frac{a_{00}+a_{10}}{\sqrt{2}}|+\rangle|0\rangle + \frac{a_{01}+a_{11}}{\sqrt{2}}|+\rangle|1\rangle)$ y

$|\psi_2'\rangle = c_2'(\frac{a_{00}-a_{10}}{\sqrt{2}}|-\rangle|0\rangle + \frac{a_{01}-a_{11}}{\sqrt{2}}|-\rangle|1\rangle)$

En el caso especial del estado de Bell $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ la medida proporcionará uno de los dos estados $|++\rangle$ y $|--\rangle$ con la misma probabilidad $\frac{1}{2}$.

4.7 Distribución cuántica de clave con entrelazamiento

En capítulos anteriores hemos visto el protocolo de distribución cuántica de clave BB84, basado en este protocolo, Artur Ekert desarrollo un esquema que utiliza pares de fotones entrelazados que pueden ser creados por Alice, por Bob o por alguna fuente separada de ambos, incluida la espía Eve. Los fotones se distribuyen de modo que Alice y Bob terminen con un fotón de cada par cada uno.

El esquema se basa en dos propiedades del entrelazamiento.

Por un lado, los estados entrelazados están perfectamente correlacionados en el sentido de que si Alice y Bob miden los fotones, obtendrán la misma polarización vertical u horizontal con un 100 % de probabilidad. Es imposible para Alice predecir si ella (y por lo tanto Bob) obtendrán polarización vertical u horizontal.

En segundo lugar, cualquier intento de espionaje por parte de Eve destruye la correlación de tal forma que Alice y Bob pueden detectarla.

El protocolo comienza con la creación de una secuencia de pares de cúbits, todos en el estado entrelazado $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$. Alice recibe el primer cúbit de cada par, mientras que Bob recibe el segundo. Cuando desean crear una clave secreta, para cada cúbit, ambos, de forma independiente y aleatoria, eligen la base estándar $|0\rangle, |1\rangle$ o la base Hadamard $|+\rangle, |-\rangle$ en la que medir, al igual que en el protocolo BB84. A continuación, y una vez que han realizado sus medidas, comparan las bases y descartan

aquellos bits en los que sus bases difieren.

Si Alice mide el primer cúbit en la base estándar y obtiene $|0\rangle$, entonces todo el estado se convierte en $|00\rangle$. Si Bob ahora mide en la base estándar, obtiene el resultado $|0\rangle$ con certeza. Sin embargo, si mide en la base de Hadamard, obtiene $|+\rangle$ y $|-\rangle$ con igual probabilidad, ya que $|00\rangle = |0\rangle(\frac{1}{\sqrt{2}}(|+\rangle + |-\rangle))$. Al igual que en el protocolo BB84, interpreta los estados$|+\rangle$ y $|-\rangle$ como correspondientes a los valores de bits clásicos 0 y 1 respectivamente; así, cuando mide en la base $|+\rangle, |-\rangle$ y Alice mide en la base estándar, obtiene el mismo valor de bit que Alice solo la mitad de las veces. El comportamiento es similar cuando la medición de Alice indica que su cúbit está en el estado $|1\rangle$. Sin embargo, si Alice mide en la base de Hadamard y obtiene el resultado de que su cúbit está en el estado $|+\rangle$, todo el estado se convierte en $|+\rangle|+\rangle$. Si Bob ahora mide en la base de Hadamard, obtiene $|+\rangle$ con certeza, mientras que si mide en la base estándar obtiene $|0\rangle$ y $|1\rangle$ con la misma probabilidad. Dado que siempre obtienen el mismo valor si miden en la misma base, el protocolo da como resultado una clave aleatoria compartida, siempre que los pares iniciales sean pares entrelazados o pares EPR (De Einstein Podolsky Rosen). La seguridad del esquema se basa en agregar pasos al protocolo que acabamos de describir que permiten a Alice y Bob probar la fidelidad de sus pares EPR.

4.8 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