Computación Cuántica

Chenjie Huang

Índice

1. Introducción

Alguna breve introducción y tal???

1.1. Objetivos

(Pendiente)

- Introducción a la computación cuántica. Como la metodología de trabajo. Teoría matemática, espacios de Hilbert y Producto tensorial.
- Estructura básica, qubits, y puertas cuánticas.
- Algoritmos cuánticos. Con ejemplos en qiskit.
  - Algoritmo de Deutsch
  - Algoritmo de Deutsch-Jozsa
  - Algoritmo de Búsqueda de Grover
  - Algoritmo de Periodicidad de Simon
  - Algoritmo de Factorización de Shor.

1.2. Metodología

Lectura parcial de los libros que ha recomendado el tutor, seguidos de su discusión e implementación en Qiskit.(?)

2. Preliminares

La Teoría Cuántica se apoya principalmente sobre álgebra lineal, concretamente sobre el espacio vectorial complejo de dimensión finita $\mathbb{C}^n$. En esta sección que servirá como preliminares como indica el título, nos centraremos en la teoría de álgebra lineal sobre el espacio vectorial complejo.

El objetivo es conseguir que este apartado sirva a modo de fundamento y bases para secciones posteriores y también de consulta posteriormente.

2.1. Espacios Vectoriales

Definición 2.1 *Un espacio vectorial sobre un cuerpo $\mathbb{K}$ es un conjunto no vacío $\mathbb{V}$, cuyo elementos llamaremos vectores, y llevan asociado dos operaciones,*

- *La Suma, $+ : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{V}$*
- *El Producto por un escalar, $\cdot : \mathbb{K} \times \mathbb{V} \longrightarrow \mathbb{V}$*

*tal que $(\mathbb{V}, +)$ cumple las propiedades de formar un **grupo abeliano** y el producto por un escalar $\cdot$ cumpla las propiedades de:*

- *Existencia de elemento neutro:*

$$\exists e \in \mathbb{K} \text{ tal que } \forall v \in \mathbb{V}, e \cdot v = v \tag{2.1}$$

- *Propiedad asociativa:*

$$\forall a, b \in \mathbb{K}, \forall v \in \mathbb{V}, a \cdot (b \cdot v) = (a \cdot b) \cdot v \tag{2.2}$$

- *Propiedad distributiva respecto a la suma de vectores:*

$$\forall a \in \mathbb{K}, \forall u, v \in \mathbb{V}, a \cdot (u + v) = a \cdot u + a \cdot v \tag{2.3}$$

- *Propiedad distributiva respecto a la suma de escalares:*

$$\forall a, b \in \mathbb{K}, \forall v \in \mathbb{V}, (a+b) \cdot v = a \cdot v + b \cdot v \tag{2.4}$$

En el caso de que el cuerpo de escalares sea el de los complejos $\mathbb{C}$, se le denominará **espacio vectorial complejo**, siendo estas de gran interés para nuestro campo de estudio que es la mecánica cuántica.

A partir de ahora usaremos $\mathbb{C}$ como cuerpo de escalares del espacio vectorial junto a la notación estándar de mecánica cuántica para referirnos a los elementos básicos de la álgebra lineal.

Denotaremos al vector en un espacio vectorial $\mathbb{V}$ como $|v\rangle$, donde usaremos $|\cdot\rangle$ para indicar que es un vector del espacio, denominado ***ket***.

En cuanto al elemento neutro del espacio vectorial, el vector cero, lo denotaremos excepcionalmente como $\mathbf{0}$. Veremos posteriormente que usaremos $|0\rangle$ para referirnos a algo completamente diferente.

Centrándonos más en $\mathbb{C}^n$, el espacio vectorial complejo cuyo elementos son n-tuplas $(z_1, z_2, \dots z_n)$, usaremos a veces la notación de vector columna:

$$\begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_n \end{bmatrix}$$

2.2. Bases y dimensión

Definición 2.2 *Sea $|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle$ vectores de un cierto espacio vectorial $\mathbb{V}$ sobre $\mathbb{C}$. Diremos que un vector $|v\rangle \in \mathbb{V}$ es **combinación lineal** de ellos si existen $a_1, a_2, \dots, a_n \in \mathbb{C}$ escalares tal que podemos escribir $|v\rangle$ como:*

$$|v\rangle = \sum_{i=1}^{n} a_i \cdot |v_i\rangle \tag{2.5}$$

Definición 2.3 *Sea $\{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$ un conjunto de vectores de un cierto espacio vectorial $\mathbb{V}$ sobre $\mathbb{C}$. Diremos que son **linealmente dependientes** si existen $a_1, a_2, \dots, a_n \in \mathbb{C}$, con algún $a_i \neq 0$, tal que*

$$a_1 |v_1\rangle + a_2 |v_2\rangle + \dots + a_n |v_n\rangle = 0 \tag{2.6}$$

*Además diremos que son **linealmente independientes** si no son linealmente dependientes. Es decir, si existe una combinación lineal de ellos, entonces los coeficientes son todos nulos.*

Definición 2.4 *Llamaremos entonces al conjunto $B = \{|v_1\rangle, |v_2\rangle, \dots, |v_n\rangle\}$ **base** del espacio $\mathbb{V}$ si:*

- *B es linealmente independiente.*
- *$\forall |v\rangle \in \mathbb{V}$, $|v\rangle$ puede ser escrito como combinación lineal de vectores de B.*

Además podemos asegurar la existencia de este conjunto para todo espacio vectorial. Y también de que el número de elementos de dos bases distintas del mismo espacio vectorial coincide y nos referiremos a este número como **dimensión** del espacio $\mathbb{V}$.

Como hemos hecho mención antes, nuestro interés se halla en espacios vectoriales de dimensión finita, por tanto haremos omiso de las cuestiones relacionadas con espacios de dimensión infinita.

2.3. Aplicaciones lineales y forma matricial

Definición 2.5 *Una aplicación lineal entre dos espacios vectoriales $\mathbb{V}$ y $\mathbb{W}$ sobre el mismo cuerpo $\mathbb{C}$ es una aplicación $f : \mathbb{V} \longrightarrow \mathbb{W}$ tal que es lineal sobre sus componentes, es decir, si $|v\rangle = \sum_{i=1}^{n} a_i \cdot |v_i\rangle$ entonces se cumple:*

$$f(|v\rangle) = f(\sum_{i=1}^{n} a_i \cdot |v_i\rangle) = \sum_{i=1}^{n} a_i \cdot f(|v_i\rangle) \tag{2.7}$$

Diremos además que una aplicación lineal está definida sobre $\mathbb{V}$ para referirnos a que es una aplicación lineal de $\mathbb{V}$ a $\mathbb{V}$

Un aplicación de gran importancia es la aplicación identidad, que denotaremos con $id_{\mathbb{V}}$ y cumple la propiedad de que $\forall |v\rangle \in \mathbb{V}$, $id_{\mathbb{V}}(|v\rangle) = |v\rangle$.

Observando la expresión 2.7 podemos llegar a la conclusión de que una aplicación lineal está completamente determinada por su acción sobre los elementos de una base, pues todo vector se puede expresar como combinación lineal de los vectores de una base.

Una manera muy útil de expresar una aplicación lineal es a través de su expresión matricial. Veamos esto con la aplicación de $f : \mathbb{V} \longrightarrow \mathbb{W}$ sobre los vectores de las bases correspondientes. Sea $\{|v_1\rangle, \ldots, |v_m\rangle\}$ y $\{|w_1\rangle, \ldots, |w_n\rangle\}$ bases correspondientes a $\mathbb{V}$ y $\mathbb{W}$.

Entonces para cada j de 1 a m existirán $a_{1j}, \ldots, a_{nj} \in \mathbb{C}$ tal que

$$f(|v_j\rangle) = \sum_{i=1}^{n} a_{ij} |w_i\rangle \tag{2.8}$$

por ser $f(|v_j\rangle) \in \mathbb{W}$ y $\{|w_1\rangle, \ldots, |w_n\rangle\}$ base de $\mathbb{W}$.

Definición 2.6 *Llamaremos entonces A a la matriz formada por los elementos a_{ij} de la ecuación 2.8 en la posición (ij) en la matriz, como representación matricial de la función f.*

Además, tomando las **coordenadas z_j** de un vector $|v\rangle = \sum_{j=1}^{m} z_j |v_j\rangle$ de $\mathbb{V}$ y su imagen por f con la expresión 2.8:

$$f(|v\rangle) = f(\sum_{j=1}^{m} z_j |v_j\rangle) = \sum_{j=1}^{m} z_j f(|v_j\rangle) = \sum_{j=1}^{m} z_j (\sum_{i=1}^{n} a_{ij} |w_i\rangle) = \sum_{i=1}^{n} (\sum_{j=1}^{m} a_{ij} z_j) |w_i\rangle \tag{2.9}$$

podemos observar la aplicación de f sobre el vector $|v\rangle$ no es más que el producto de la matriz A con el vector $|v\rangle$ en columnas:

$$A |v\rangle = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1m} \\ a_{21} & a_{22} & \ldots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nm} \end{bmatrix} \begin{bmatrix} z_1 \\ z_2 \\ \vdots \\ z_m \end{bmatrix} = \begin{bmatrix} \sum_{j=1}^{m} a_{1j} z_j \\ \sum_{j=1}^{m} a_{2j} z_j \\ \vdots \\ \sum_{j=1}^{m} a_{nj} z_j \end{bmatrix} \tag{2.10}$$

2.4. Producto Escalar y Espacios de Hilbert

Definición 2.7 *Un **producto escalar**, o también conocido como producto interno, es una aplicación $(\cdot, \cdot) : \mathbb{V} \times \mathbb{V} \longrightarrow \mathbb{C}$ que cumple:*

- *Es definida positiva,*

$$(|v\rangle, |v\rangle) \geq 0 \tag{2.11}$$

  y

$$(|v\rangle, |v\rangle) = 0 \Leftrightarrow |v\rangle = 0 \tag{2.12}$$

- *Es lineal en el primer argumento y lineal conjugada en el segundo,*

$$(a |u\rangle + b |v\rangle, |w\rangle) = \bar{a} \cdot (|u\rangle, |w\rangle) + \bar{b} \cdot (|v\rangle, |w\rangle) \tag{2.13}$$

$$(|u\rangle, a |v\rangle + b |w\rangle) = a \cdot (|u\rangle, |v\rangle) + b \cdot (|u\rangle, |w\rangle) \tag{2.14}$$

- *Es anti-simétrico,*

$$(|u\rangle, |v\rangle) = \overline{(|v\rangle, |u\rangle)} \tag{2.15}$$

donde $a, b \in \mathbb{C}$, $|u\rangle, |v\rangle, |w\rangle \in \mathbb{V}$ y $\bar{a} \in \mathbb{C}$ es el conjugado complejo del elemento a.

La notación estándar del producto escalar en mecánica cuántica no es $(|u\rangle, |v\rangle)$, sino $\langle u|v\rangle$, donde $|u\rangle$ y $|v\rangle$ son vectores de $\mathbb{V}$ y $\langle u|$ denota el vector dual al vector $|u\rangle$, también conocido como **bra**. El dual es una aplicación lineal cuya definición es $\langle u| (|v\rangle) := \langle u|v\rangle = (|u\rangle, |v\rangle)$. A partir de ahora, usaremos más esta notación.

Definición 2.8 *Diremos que dos vectores $|u\rangle$ y $|v\rangle$ son* ***ortogonales*** *si su producto escalar es 0.*
Además definiremos como ***norma*** *del vector como*

$$\||v\rangle\| = \sqrt{\langle v|v\rangle} \tag{2.16}$$

y diremos que $|v\rangle$ es unitario o normalizado si $\||v\rangle\| = 1$.

Definición 2.9 *Por tanto diremos que un conjunto, $|i\rangle \in \mathbb{V}$ de vectores es* ***ortonormal*** *si son vectores unitarios y además son ortogonales entre sí. Es decir,*

$$\forall\, |i\rangle, |j\rangle \in \mathbb{V}\ \langle i|j\rangle = \delta_{ij} = \begin{cases} 1 & si \quad i = j \\ 0 & si \quad i \neq j \end{cases} \tag{2.17}$$

Un espacio vectorial euclídeo no es más que un espacio vectorial dotado de un producto escalar. Trabajaremos a partir de ahora en un espacio vectorial complejo de dimensión finita y con un producto escalar. Dicho espacio es denominado usualmente como **espacio de Hilbert**.

Definición 2.10 ***Espacio de Hilbert*** *(falta)(y buscar referencia)*

En nuestro caso por la finitud de la dimensión, un espacio de Hilbert es equivalente a espacio euclídeo. No entraremos en detalles en el caso de que la dimensión sea infinita, ya que para hablar de espacio de Hilbert sería necesario que se cumplan alguna propiedad extra. Nos centraremos en el caso de la dimensión finita cuando hablemos de espacio de Hilbert.

Podemos ver ahora que el producto escalar en un espacio de Hilbert tiene una representación matricial muy útil. Consideramos $|u\rangle = \sum_i u_i |i\rangle$ y $|v\rangle = \sum_j v_j |j\rangle$ con $|i\rangle, |j\rangle$ vectores de una base ortonormal $\{|1\rangle, |2\rangle, \ldots, |n\rangle\}$. Entonces el producto escalar,

$$\langle u|v\rangle = (\sum_i u_i |i\rangle, \sum_j v_j |j\rangle) = \sum_{ij} \bar{u_i} v_j \langle i|j\rangle = \sum_{ij} \bar{u_i} v_j \delta_{ij} = \sum_i \bar{u_i} v_i \tag{2.18}$$

que claramente es el producto entre un vector fila conjugado y uno columna,

$$\langle u|v\rangle = [\bar{u_1}\bar{u_2}\ldots\bar{u_n}] \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = \sum_i \bar{u_i} v_i \tag{2.19}$$

Podemos observar también que el vector dual $\langle u|$ se puede expresar como un vector fila cuyas componentes están conjugadas.

Una manera útil de ver las aplicaciones lineales es a través de su representación como **producto exterior**.

Definición 2.11 *Llamaremos producto exterior a la aplicación $|u\rangle\langle v| : \mathbb{V} \longrightarrow \mathbb{W}$, donde $|v\rangle \in \mathbb{V}$ y $|u\rangle \in \mathbb{W}$,*

$$|u\rangle\langle v|(|v'\rangle) = |u\rangle\langle v|v'\rangle = \langle v|v'\rangle \cdot |u\rangle \tag{2.20}$$

Considerando ahora una base ortonormal $\{|i\rangle\}_{1\leq i\leq n}$, podemos deducir la propiedad de completitud del producto exterior. Sea el vector $|v\rangle = \sum_i v_i |i\rangle$, teniendo en cuenta que $\langle i|v\rangle = v_i$, tenemos que la aplicación de $\sum_i |i\rangle\langle i|$ sobre el vector

$$(\sum_i |i\rangle\langle i|)(|v\rangle) = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i |i\rangle = |v\rangle \tag{2.21}$$

Lo que nos permite llegar a la conclusión de que $\sum_i |i\rangle\langle i|$ es equivalente a la identidad.

Teniendo en mente esta propiedad podemos conseguir la expresión de un aplicación lineal $f : \mathbb{V} \longrightarrow \mathbb{W}$, considerando $|v_i\rangle$ y $|w_j\rangle$ un base ortonormal de ambos espacios. Con la propiedad de completitud tenemos que

$$f \equiv id_{\mathbb{W}} \circ f \circ id_{\mathbb{V}} \equiv \sum_{ij} (|w_j\rangle\langle w_j|) \circ f \circ (|v_i\rangle\langle v_i|) \equiv \sum_{ij} \langle w_j|f(v_i)\rangle |w_j\rangle\langle v_i| \tag{2.22}$$

donde podemos concluir que el valor $\langle w_j|f(v_i)\rangle$ es el elemento de la columna i y fila j de la representación matricial de f en las bases correspondientes.

Además observamos que esto concuerda con la expresión de un vector y su dual como vector fila y columna pues el producto resultante de

$$\begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} [v_1 \dots v_n] = \begin{bmatrix} w_1 v_1 & \dots & w_1 v_n \\ \vdots & \ddots & \vdots \\ w_n v_1 & \dots & w_n v_n \end{bmatrix} \tag{2.23}$$

es una matriz, correspondiente a la aplicación lineal.

2.5. Matrices Adjuntas o Hermitianas

Veremos ahora un tipo de matriz y su función asociada que se comporta de una manera muy buena con el espacio de Hilbert.

Definición 2.12 *Consideramos una matriz $A \in \mathbb{C}^{n\times n}$, definiremos su **adjunta** o **conjugada Hermitiana** como la matriz traspuesta con los elementos conjugados y lo denotaremos como $A^\dagger = \overline{A^T}$*

*Además diremos que A es **hermintiana** si $A^\dagger = A$ y llamaremos a la aplicación lineal asociada, aplicación **auto-adjunta**.*

Podemos ver fácilmente que este tipo de matrices cumplen ciertas propiedades,

- $\forall\, |u\rangle, |v\rangle \in \mathbb{V}$
$$(|u\rangle, A\,|w\rangle) = (A^\dagger\,|u\rangle, |w\rangle) \tag{2.24}$$
- Definiremos por convenio la adjunta de un vector $|v\rangle^\dagger = \langle v|$, que concuerda con toda la notación que hemos estado usando. De esta manera, teniendo en cuenta que $(AB)^\dagger = B^\dagger A^\dagger$, tenemos que
$$(A\,|v\rangle)^\dagger = \langle v|\, A^\dagger \tag{2.25}$$

Otras matrices que nos interesan son las matrices **unitarias**. Son un tipo de matrices invertibles que cumplen que

$$U * U^\dagger = U^\dagger * U = I_n \tag{2.26}$$

2.6. Producto Tensorial

En esta sección estudiaremos el producto tensorial entre espacios vectoriales, una herramienta esencial para trabajar con sistemas cuánticos de varios elementos en esta área. Hablaremos de estos sistemas en secciones posteriores, por ahora nos centraremos en el producto tensorial.

Definición 2.13 *Consideramos $\mathbb{V}$ y $\mathbb{W}$ dos espacios vectoriales, llamaremos **producto escalar** a la aplicación bilineal $\otimes : \mathbb{V}\times\mathbb{W} \longrightarrow \mathbb{V}\otimes\mathbb{W}$, que lleva $|v\rangle \in \mathbb{V}$ y $|w\rangle \in \mathbb{W}$ a un elemento de $\mathbb{V}\otimes\mathbb{W}$ que llamaremos **tensor** y lo denotaremos por $|v\rangle \otimes |w\rangle$, o de manera abreviada $|v\rangle\,|w\rangle$, $|vw\rangle$.*

Además esta aplicación cumple las siguientes propiedades:

- Sea z un escalar y $|v\rangle$ y $|w\rangle$ elementos de $\mathbb{V}$ y $\mathbb{W}$ respectivamente,
$$z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z\,|w\rangle) \tag{2.27}$$
- Para $|v_1\rangle$, $|v_2\rangle \in \mathbb{V}$ y $|w\rangle \in \mathbb{W}$ se tiene,
$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle \tag{2.28}$$
- Para $|v\rangle \in \mathbb{V}$ y $|w_1\rangle$, $|w_2\rangle \in \mathbb{W}$ se tiene,
$$(|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle \tag{2.29}$$

El espacio de la imagen sigue siendo un espacio vectorial y de hecho, si tomamos $\{|v_1\rangle, \ldots, |v_m\rangle\}$ y $\{|w_1\rangle, \ldots, |w_n\rangle\}$ como bases de $\mathbb{V}$ y $\mathbb{W}$ respectivamente, tenemos que

$$\{|v_i\rangle \otimes |w_j\rangle \mid 1 \leq i \leq m, 1 \leq j \leq n\} \tag{2.30}$$

es una base de $\mathbb{V} \otimes \mathbb{W}$. Y por tanto, la dimensión como espacio vectorial de $\mathbb{V} \otimes \mathbb{W}$ es $m \cdot n$ siendo m y n la dimensión de $\mathbb{V}$ y $\mathbb{W}$ respectivamente.

Las aplicaciones lineales del espacio $\mathbb{V}\otimes\mathbb{W}$ que consideraremos serán aquellas resultantes del producto tensorial de dos aplicaciones lineales del espacio de los factores, de manera que cumplan

$$(f \otimes g)(|v\rangle \otimes |w\rangle) = f(|v\rangle) \otimes g(|w\rangle). \tag{2.31}$$

De hecho, toda aplicación lineal de $\mathbb{V} \otimes \mathbb{W}$ se puede representar como combinación lineal de aplicaciones de $\mathbb{V}$ y $\mathbb{W}$ con el producto tensorial, actuando como espacio resultante del producto tensorial del espacio de los endomorfismos.

En cuanto a la práctica resulta muy cómodo trabajar con la representación matricial de estas aplicaciones y el producto de Kronecker. Pues si consideramos A una matriz $m \times n$ y B una matriz $p \times q$, su producto tensorial sería:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \ldots & a_{1n}B \\ a_{21}B & a_{22}B & \ldots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \ldots & a_{mn}B \end{bmatrix} \tag{2.32}$$

donde a_{ij} es el elemento de la posición (ij) de la matriz A.

De la misma manera se puede operar con los vectores columnas del espacio vectorial $\mathbb{C}^n$. Por ejemplo, si tenemos $|v\rangle\, y\, |w\rangle$ vectores de $\mathbb{C}^n$ y $v_1, v_2, \ldots, v_n$, $w_1, w_2, \ldots, w_n$ sus coordenadas respectivamente en una base. Entonces su producto tensorial en forma matricial sería,

$$\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} \otimes \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} v_1 \cdot \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \\ v_2 \cdot \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \\ \vdots \\ v_n \cdot \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \end{bmatrix} = \begin{bmatrix} v_1w_1 \\ v_1w_2 \\ \vdots \\ v_1w_n \\ v_2w_1 \\ v_2w_2 \\ \vdots \\ v_2w_n \\ v_nw_1 \\ v_nw_2 \\ \vdots \\ v_nw_n \end{bmatrix} \tag{2.33}$$

3. Estructuras y Puertas Cuánticas

En esta sección veremos el sistema de información en el que se basa la computación cuántica y su representación matemática. Igual que en la computación clásica se basa en el concepto de bit, en la computación cuántica se estudiará el **bit cuántico** o **qubit** (de quantum bit en inglés). Es verdad que el qubit, al igual que el bit, son objetos físicos de un sistema físico real como partículas subatómicas en un ordenador cuántico. Pero nosotros nos centraremos en describir el qubit como un objeto matemático abstracto con ciertas propiedades determinadas.

3.1. Qubit

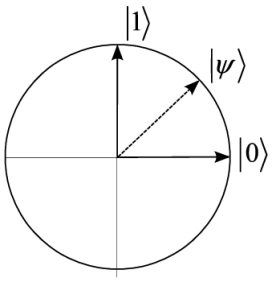
Conocemos el concepto de bit, que es un elemento de un sistema con dos estados posibles. Estos dos estados son generalmente denominados como "verdadero.º "falso, o incluso con 0 o 1.

Definición 3.1 *Entonces llamaremos* ***qubit*** *al objeto matemático con dos posibles estados correspondientes al bit clásico* $|0\rangle$ *y* $|1\rangle$*, además de una combinación lineal de estos dos estados que llamaremos como* ***superposición****:*

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

Con α *y* β *números complejos que cumplen que* $|\alpha|^2 + |\beta|^2 = 1$*.*

Se entiende fácilmente el estado de un qubit como un vector del espacio vectorial complejo de dimensión 2, restringido a la circunferencia unidad, donde los estados $|0\rangle$ y $|1\rangle$ son los elementos de la base ortonormal del espacio con α y β como coordenadas del vector de norma 1.



Podemos determinar el estado de un bit clásico a la hora de examinarlo, pero en el caso del qubit, no podemos determinar el estado cuántico de un qubit en superposición, es decir, no podemos hallar el valor de α y β. Lo que sí podemos hacer es **medir** el qubit, determinar si colapsa en el estado $|0\rangle$ con probabilidad $|\alpha|^2$ ó en el estado $|1\rangle$ con probabilidad $|\beta|^2$. En otra palabras, el proceso de medir un qubit, nos devuelve como salida un estado clásico al que colapsa y deja de estar en superposición de varios estados de manera simultanea.

Veamos ahora otra representación geométrica del qubit que puede resultar útil. Consideramos un qubit en estado de superposición.

$$|\psi\rangle = c_0\,|0\rangle + c_1\,|1\rangle \tag{3.2}$$

con $\|c_0|^2 + |c_1|^2 = 1$. Reescribimos la expresión en coordenadas en forma exponencial de un número complejo,

$$|\psi\rangle = r_0 e^{i\varphi_0}\,|0\rangle + r_1 e^{i\varphi_1}\,|1\rangle \tag{3.3}$$

Lo multiplicamos por un escalar de módulo 1, así no alteramos su estado cuántico,

$$e^{-i\varphi_0}\,|\psi\rangle = e^{-i\varphi_0}(r_0 e^{i\varphi_0}\,|0\rangle + r_1 e^{i\varphi_1}\,|1\rangle) = r_0\,|0\rangle + r_1 e^{i(\varphi_1-\varphi_0)}\,|1\rangle \tag{3.4}$$

Tomando ahora coordenadas polares $r_0 = \cos(\theta)$, $r_1 = \sin(\theta)$ y el cambio de variables $\varphi = \varphi_1 - \varphi_0$, resulta en la siguiente expresión,

$$|\psi\rangle = \cos(\theta)\,|0\rangle + e^{i\varphi}\sin(\theta)\,|1\rangle \tag{3.5}$$

Considerando θ y φ como coordenadas de un punto en una esfera tridimensional, podemos ver el estado del qubit como un punto en la superficie de dicha esfera, siendo los polos los estados $|0\rangle$ y $|1\rangle$. Esta esfera recibe el nombre de **esfera de Bloch** y veremos en poco que con ella podemos representar operaciones de qubits como rotaciones de la esfera.

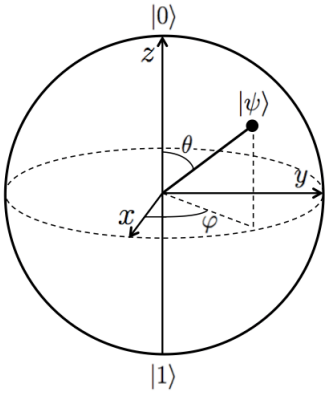


Figura 1: Esfera de Bloch.

3.2. Sistema de Varios Qubits

Tomamos interés en un sistema de un número mayor de qubits, que enlazaremos a través del producto tensorial de los espacios vectoriales. Por tanto un elemento de él estará representado por un vector de $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \ldots \otimes \mathbb{C}^2$ que denotaremos como $(\mathbb{C}^2)^{\otimes n}$ donde n es el número de qubits del sistema y cuya dimensión como espacio vectorial es 2^n

Por ejemplo, si queremos un sistema de 2 qubits en comparación a los estados clásicos de un bit tendríamos 00, 01, 10 y 11, por tanto nuestro sistema de 2 qubits tendría los estados $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$ que se corresponden con el producto tensorial del estado de los dos qubits $|x\rangle \otimes |y\rangle$ con $x, y \in \{0, 1\}$. Vamos a trabajar más cómodamente con coordenadas del vector en su expresión matricial, consideramos primero,

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \ |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{3.6}$$

Como hemos visto en la sección anterior, aplicaremos el producto de Kroner para obtener las expresiones matriciales de $|00\rangle$, $|01\rangle$, $|10\rangle$ y $|11\rangle$,

$$|00\rangle = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \ |01\rangle = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \ |10\rangle = \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \ |11\rangle = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{3.7}$$

Observamos que forman una base ortonormal de un espacio vectorial de dimensión $2^2 = 4$ y que además cada coordenada corresponde a un estado clásico del qubit:

$$|01\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \tag{3.8}$$

Por tanto, si tomamos un sistema de dos qubits arbitrario en superposición,

$$|\psi\rangle = c_0 |00\rangle + c_1 |01\rangle + c_2 |10\rangle + c_3 |11\rangle \tag{3.9}$$

su representación matricial sería:

$$|\psi\rangle = \begin{matrix} \mathbf{00} \\ \mathbf{01} \\ \mathbf{10} \\ \mathbf{11} \end{matrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \end{bmatrix} \tag{3.10}$$

Trabajaremos a partir de ahora con la notación del sistema de varios qubits como $|xy\rangle$, $|x \otimes y\rangle$, ó $|x\rangle \otimes |y\rangle$ y los trataremos de manera indiferente según convenga.

Podemos medir únicamente un subconjunto de qubits del sistema total siendo la probabilidad de obtener el qubit en un estado concreto la suma de las probabilidades del estado del sistema con el qubit correspondiente en el estado en concreto. Por ejemplo si tomamos el sistema de dos qubits anterior, la probabilidad de que el primer qubit esté en el estado $|0\rangle$ será $|c_0|^2 + |c_1|^2$ que son las probabilidades de que el sistema esté en el estado $|00\rangle$ ó $|01\rangle$. Hacemos notar que tras medirlo, el sistema quedará en el estado

$$|\psi'\rangle = \frac{c_0 |00\rangle + c_1 |01\rangle}{\sqrt{|c_0|^2 + |c_1|^2}} \tag{3.11}$$

ya que hemos determinado el estado del primer qubit haciéndolo colapsar a un estado clásico a la hora de medirlo. Además, el denominador $\sqrt{|c_0|^2 + |c_1|^2}$ se debe por normalizar el vector que representa el estado del sistema. Recordemos que esto era una condición necesaria que tenemos que pedir. Un ejemplo importante de un sistema de dos qubits es el **estado de Bell** ó **par ERP**,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.12}$$

que nos muestra una propiedad importante de los sistemas de varios qubits a la hora de hacer mediciones. Si medimos el primer qubit tendrá una probabilidad de $(\frac{1}{\sqrt{2}})^2 = \frac{1}{2}$ de estar en el estado $|0\rangle$ y una probabilidad de $\frac{1}{2}$ de estar en el estado $|1\rangle$. Esto dejará el sistema en el estado $|\psi'\rangle = |00\rangle$ ó $|\psi'\rangle = |11\rangle$. En cualquier caso tenemos que ambas situaciones, tras medir el primer qubit, si medimos el segundo este coincidirá con el primero. Es decir, que ambos qubits está relacionados(entagled).

Nos fijamos un momento en la dimensión del espacio vectorial que representa nuestro sistema. Supongamos que tenemos un número de un tamaño considerable de qubits, $n = 500$. Si quisiéramos simular este sistema en un ordenador clásico realizando las operaciones matriciales necesarias en la computación, tendríamos que para un estado del sistema almacenar 2^{500} coordenadas complejas del vector además de trabajar con matrices de tamaño 2^{500}. Esto claramente no es factible hoy en día resultando en una de los problemas en cuanto a la computación cuántica.

3.3. Circuitos y Puertas Cuánticas

Al igual que un circuito de un ordenador clásico consiste en cables y puertas lógicas que interaccionan con la información que es transportada por el cableado, un circuito cuántico consiste en cables que transportan información cuántica en forma de qubits que son manipulados a través de puertas cuánticas.

Consideremos primero la puerta clásica **NOT** que queremos que realice la operación de la tabla de verdad sobre un bit, es decir,

$$\begin{cases} 0 \to 1 \\ 1 \to 0 \end{cases} \tag{3.13}$$

intercambiando los estados 0 y 1. Queremos que nuestra puerta cuántica se comporte de la misma manera sobre qubits. Queremos que intercambie los estados $|0\rangle$ y $|1\rangle$ y además por ser puerta cuántica pediremos que sea lineal, es decir, si tenemos un un qubit arbitrario en estado de superposición

$$\alpha |0\rangle + \beta |1\rangle \tag{3.14}$$

queremos que se aplique de forma lineal a cada uno de los términos de la suma,

$$\alpha |1\rangle + \beta |0\rangle . \tag{3.15}$$

Igual que hemos asociado con vectores a los bits, y podemos operar con los vectores de forma matricial, las puertas lógicas están asociados a las matrices. Por tanto si tomamos la matriz $\text{NOT} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, esta matriz cumple que

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \text{ y } \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \tag{3.16}$$

tomando el vector correspondiente al estado cuántico $|0\rangle$ y $|1\rangle$ y los intercambia:

$$\text{NOT} |0\rangle = |1\rangle \text{ y NOT} |1\rangle = |0\rangle \tag{3.17}$$

Otra propiedad que les pediremos a las puertas cuánticas es que sean reversibles. Esto es que dados la salida y la operación aplicada seamos capaces de determinar la entrada del circuito. Representaremos las puertas cuánticas con matrices unitarias que son reversibles por su propia adjunta. Recordemos que esto es:

$$U * U^{\dagger} = U^{\dagger} * U = I_n \tag{3.18}$$

Podemos poner de ejemplo, la operación AND, que toma dos bits y nos devuelve 1 si ambos inputs son 1. Esta operación no es reversible, ya que si conocemos solamente el output, no podemos determinar cuál ha sido el input de la operación.
De esta manera tenemos que, aparte de la propiedad de ser lineal que está implicada, cualquier matriz unitaria lleva asociada su puerta cuántica correspondiente, siendo el único requisito que pediremos. Veamos otras puertas cuánticas de un qubits de importancia. Si consideramos las matrices de Pauli,

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \tag{3.19}$$

tendremos que cada una de ellas tiene asociado una puerta cuántica correspondiente. De hecho, la matriz X corresponde con la puerta NOT. Podemos evaluar la matriz con los estados del qubit para determinar su comportamiento, pues por ejemplo si tomamos la matriz Z,

$$Z(\alpha\,|0\rangle + \beta\,|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \alpha\,|0\rangle - \beta\,|1\rangle\,, \tag{3.20}$$

que cambia el signo del coeficiente de $|1\rangle$.
Otra manera de visualizar estas puertas es como rotaciones de 180º sobre la esfera de Bloch en el eje correspondiente.

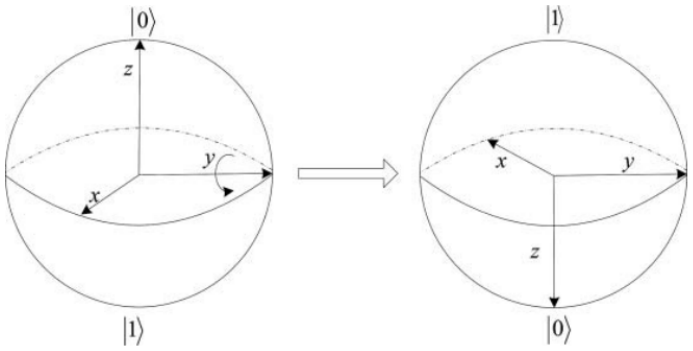


Figura 2: Rotación sobre el eje Y en la esfera de Bloch.

Una puerta cuántica de mucha importancia es la puerta de Hadamard ya que nos permitirá poner qubit en una configuración en la que todos los estados son equiprobables. Esta puerta tiene por matriz:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \tag{3.21}$$

que lleva

$$\begin{cases} |0\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle \to \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{cases} \tag{3.22}$$

Una propiedad que cumple $H^2 = I$ que se comprueba fácilmente. Esto nos permite posteriormente llevar estados $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ a $|0\rangle$, lo que usaremos posteriormente en los algoritmos.

Ya hemos mencionado que es posible visualizar las puertas cuánticas como rotaciones en la esfera de Bloch, por ejemplo si tomamos la expresión de un estado de un qubit en polares,

$$|\psi\rangle = \cos(\theta)\,|0\rangle + e^{i\varphi}\sin(\theta)\,|1\rangle\,, \tag{3.23}$$

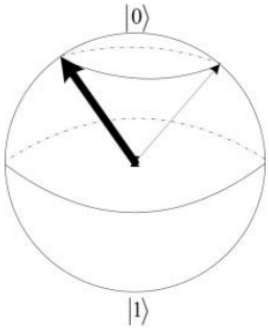
y le aplicamos la siguiente matriz

$$R(\omega) = \begin{bmatrix} 1 & 0 \\ 0 & e^{\omega} \end{bmatrix} \tag{3.24}$$

obteniendo como resultado:

$$|\psi'\rangle = \cos(\theta)\,|0\rangle + e^{\omega}e^{i\varphi}\sin(\theta)\,|1\rangle = \cos(\theta)ket0 + e^{i\varphi+\omega}\sin(\theta)\,|1\rangle \tag{3.25}$$

de esta manera hemos conseguido rotar la esfera alrededor del eje Z, por lo que no hemos variado lo que podemos considerar como latitud, sino hemos variado su longitud. Este tipo de operaciones se denominan **cambios de fase**, ya que sólo estamos alterando el valor del parámetro $e^{i\varphi}$. Observamos que esta alteración de la fase del estado del qubit no produce cambios en cuanto a la medición del mismo, ya que la probabilidad de que un qubit colapse en un estado clásico depende en este caso únicamente del parámetro θ, su latitud en la esfera de Bloch.



Otras rotaciones, por ejemplos si queremos rotar la espera un cierto ángulo ω respecto a un eje, tendría la siguiente expresión:

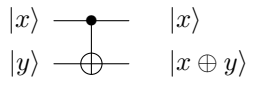
$$\begin{cases} R_x(\omega) = \cos(\frac{\omega}{2})I - i\sin(\frac{\omega}{2})X = \begin{bmatrix} cos(\frac{\omega}{2}) & -i\sin(\frac{\omega}{2}) \\ -i\sin(\frac{\omega}{2}) & \cos(\frac{\omega}{2}) \end{bmatrix} \\ R_y(\omega) = \cos(\frac{\omega}{2})I - i\sin(\frac{\omega}{2})Y = \begin{bmatrix} cos(\frac{\omega}{2}) & -\sin(\frac{\omega}{2}) \\ \sin(\frac{\omega}{2}) & \cos(\frac{\omega}{2}) \end{bmatrix} \\ R_z(\omega) = \cos(\frac{\omega}{2})I - i\sin(\frac{\omega}{2})Z = \begin{bmatrix} e^{-i\omega/2} & 0 \\ 0 & e^{i\omega/2} \end{bmatrix} \end{cases} \tag{3.26}$$

También podemos realizar rotaciones respecto de un vector dado, consideramos $D = (D_x, D_y, D_z)$ un vector arbitrario de módulo 1, con las coordenadas correspondientes. La matriz de la rotación estará determinada por la siguiente expresión:

$$R_D(\omega) = \cos(\frac{\omega}{2})I - i\sin(\frac{\omega}{2})(D_xX + D_yY + D_zZ) \tag{3.27}$$

Veamos ahora, puertas cuánticas que involucren más de un qubit, que a pesar de que no podremos representarlos ya en la esfera de Bloch, podemos seguir considerando su representación matricial.

Una de las puertas más importantes es la puerta **NOT controlada** o **CNOT**. Esta puerta tomará dos entradas y dará dos salidas. La primera entrada la llamaremos bit de control, es decir, controlará el bit de salida. Representaremos la puerta en la siguiente ilustración de un circuito cuántico, donde cada recta horizontal representa un cable que lleva el qubit siguiendo la lectura de izquierda a derecha. Si $|x\rangle = |0\rangle$, la salida del segundo bit $|y\rangle$ permanecerá igual. Si $|x\rangle = |1\rangle$ entonces $|y\rangle$ se le aplicará la



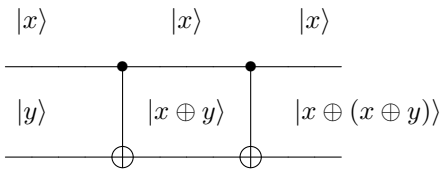
puerta NOT, es decir, será lo contrario. Es decir, realiza la siguiente transformación

$$\begin{cases} |00\rangle \to |00\rangle \\ |01\rangle \to |01\rangle \\ |10\rangle \to |11\rangle \\ |11\rangle \to |10\rangle \end{cases} \tag{3.28}$$

Esto se puede ver como que la puerta transforma un par de bits $|x, y\rangle$ en $|x, x \oplus y\rangle$, donde $\oplus$ es la operación binaria de OR excluyente, o también como la suma en módulo 2. También podemos describir la puerta CNOT con su representación matricial, considerando como base del espacio vectorial $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$,

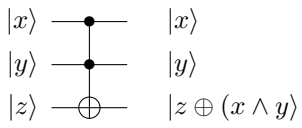
$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.29}$$

Observamos que claramente esta puerta es unitaria pues el producto por su adjunta que es ella misma resulta en la matriz identidad, pues tenemos que se cumple que $CNOT^{\dagger}CNOT = I$. Esto también se puede entender como que la puerta CNOT es reversible por ella misma:



El estado de entrada es $|x, y\rangle$ que queda trasformado en $|x, x \oplus y\rangle$ y esta última en $|x, x \oplus (x \oplus y)\rangle$. Esto es $|x, (x \oplus x) \oplus y\rangle = |x, 0 \oplus y\rangle = |x, y\rangle$, ya que $x \oplus x = 0$.

Otra puerta reversible de mucha importancia es la de Toffoli, que funciona de manera similar a la puerta NOT controlada. Trabaja con 3 bits de entrada y salida, en el que aplica la puerta NOT al último bit $|z\rangle$ si y solo si los dos anteriores tienen por estado 1, $|x, y\rangle = |11\rangle$. En otras palabras lleva el $|x, y, z\rangle$ a $|x, y, z \oplus (x \wedge y)\rangle$.

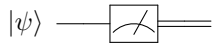


Esta puerta tiene por matriz:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \tag{3.30}$$

Ya hemos visto varias puertas que son reversibles, ahora, llamaremos puertas cuánticas a aquellas aplicaciones que actúan sobre qubits, como vectores de un espacio vectorial complejo y tendrá como representación matricial, matrices unitarias.

Una excepción de las puertas cuánticas sería la operación de medir un qubit, que se suelen realizar al final del circuito y que no son reversibles. Representaremos estas de la siguiente manera en el circuito, donde la doble recta horizontal, representa un cable que lleva información clásica, un bit.



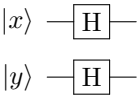
Hemos visto varios ejemplos de circuitos cuánticos con las puertas cuánticas. Vamos a centrarnos en construir circuitos más complejos combinando las puertas. Podemos tanto concatenar las puertas, realizando una operación tras otra, y operar de manera paralela con ellas, de manera simultanea a un subconjunto del sistema de qubits. Hacemos notar varias restricciones respecto al mundo clásico y es que no permitiremos bucles en los circuitos, de manera que cada circuito funcione de izquierda a derecha y sea acíclico. Además no permitiremos tanto combinar dos cableado en uno, como dividir uno en dos. Veremos en un ejemplo próximo que de hecho no podemos copiar el estado de un qubit a otro.

En cuanto a concatenar las puertas en un circuito, simplemente realizaremos una operación tras otra, de manera ordenada. Si queremos tratar la operación como una matriz, esta se representará por productos de matrices de manera natural. Por ejemplo si queremos aplicar dos veces la puerta CNOT como hemos hecho antes,

$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}=\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{bmatrix} \tag{3.31}$$

resultando lo que esperábamos, ya que la puerta CNOT es reversible por sí misma, resultando que la concatenación de ella con sigo misma es la identidad.

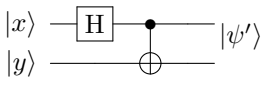
También podemos realizar operaciones de manera paralela a distintos bits a través de productos tensoriales entre las matrices, siempre cuidando el tamaño de las matrices. Por ejemplo, si queremos aplicar la puerta de Hadamard H a ambos qubits de un sistema de dos qubits, el resultado final será igual que aplicar $(H \otimes H)$ como una puerta al sistema,



Recordemos la propiedad del producto tensorial sobre las aplicaciones con la expresión 2.31, de esta manera tenemos que,

$$(H\,|x\rangle) \otimes (H\,|y\rangle) = (H \otimes H)\,|x \otimes y\rangle \tag{3.32}$$

Vamos a ver un ejemplo más de circuito en el que concatenemos la puerta CNOT con la puerta de Hadamard. Consideramos entonces el circuito:



Supongamos entonces que comenzaremos con el estado $|00\rangle$, para los otros casos el procedimiento es análogo. Entonces tendríamos que operar la siguiente expresión:

$$|\psi'\rangle = \text{CNOT} \cdot (H \otimes I)(|x \otimes y\rangle) \tag{3.33}$$

Hacemos notar que a pesar de que no le aplicamos ninguna puerta de manera simultanea a $|y\rangle$ para poder hacer el producto de matrices adecuadamente, es necesario aplicar el producto tensorial a la

puerta de Hadamard con la identidad, que no altera el estado de $|y\rangle$.
Resolvamos entonces la expresión, con el estado $|00\rangle$ en concreto. Aplicando la propiedad de la expresión 3.32 , tenemos que:

$$|\psi'\rangle = \text{CNOT} \cdot (H \otimes I)(|00\rangle) = \text{CNOT}((H\,|0\rangle) \otimes (I\,|0\rangle)) = \text{CNOT}(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle) \tag{3.34}$$

Reordenando la expresión con las propiedades del producto escalar tenemos que:

$$|\psi'\rangle = \text{CNOT}(\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)) \tag{3.35}$$

y finamente, aplicando la linealidad de CNOT:

$$|\psi'\rangle = \frac{1}{\sqrt{2}}(\text{CNOT}\,|00\rangle + \text{CNOT}\,|10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{3.36}$$

Si recordamos de la sección anterior, hemos producido con este circuito empezando en el estado $|00\rangle$ al estado de Bell que hemos visto.
Este desarrollo de naturaleza algebraica que hemos hecho, tiene su equivalente en operaciones matriciales, pues podríamos haber hecho el producto de las matrices:

$$\text{CNOT} \cdot (H \otimes I) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \tag{3.37}$$

Si operamos, obtendremos la siguiente matriz:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \tag{3.38}$$

Por tanto si operamos con $|00\rangle$, tendremos:

$$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \tag{3.39}$$

que es la expresión matricial del estado de Bell

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{3.40}$$

4. Algoritmos Cuánticos

En general, los algoritmos cuánticos siguen un esquema común entre ellos. Estos consistirán en:

- Comenzaremos con una serie de qubits en su estado clásico, es decir, $|0\rangle$ ó $|1\rangle$
- Luego, serán puestos en superposición de varios estados.
- Se le aplicarán una serie de operaciones unitarias a través de puertas cuánticas.
- Y finalmente se medirán los qubits correspondientes y según el algoritmo, se repetirá este proceso varias veces y se compararán los resultados.

4.1. Algoritmo de Deutsch

El primer algoritmo que veremos y el más simple será el algorimto de Deutsch. Este algoritmo tratará de ver si se cumple cierta propiedad para una función $f : \{0,1\} \to \{0,1\}$, concretamente si es balanceada o constante.

Definición 4.1 *Diremos que la función $f : \{0,1\} \to \{0,1\}$ es balanceada si $f(0) \neq f(1)$, y diremos que es constante si $f(0) = f(1)$.*

El algoritmo consistirá en tomar una función $f : \{0,1\} \to \{0,1\}$, con la sólo podemos evaluar la función y obtener la imagen y no sabemos cómo está definido la función y determinar si la función es balanceada o constante.

Para ello tomaremos una puerta cuántica que evaluará la función y observamos que esta tiene que ser reversible. Consideraremos la siguiente operación unitaria U_f. A esta función a veces nos referiremos como oráculo, ya que nos evaluará la función indicando la imagen sin que nosotros sepamos la definición de la función.

(Poner circuito)

En la primera entrada $|x\rangle$ será lo que queremos evaluar, y en la segunda entrada $|y\rangle$ actuará como un qubit de control. Tras el cuál, en la primera salida $|x\rangle$ permanecerá igual y en la segunda salida tendremos $|y \oplus f(x)\rangle$.

Observamos que esta puerta cuántica es reversible pues:

(Poner circuito)

El estado $|x, y\rangle$ queda trasformado en $|x, y \oplus f(x)\rangle$ y posteriormente en $|x, (y \oplus f(x)) \oplus f(x)\rangle = |x, y \oplus (f(x) \oplus f(x))\rangle = |x, y \oplus 0\rangle = |x, y\rangle$.

El circuito del algoritmo consistirá en lo siguiente:

(Poner circuito)

Esto en términos matriciales sería:

$$(H \oplus I)U_f(H \oplus H)\,|0,1\rangle = (H \oplus I)U_f(H \oplus H)\begin{bmatrix}0\\1\\0\\0\end{bmatrix} \tag{4.1}$$

Veamos en detalle el resultado al que se llega. Empezamos con el estado $|\varphi_0\rangle = |0,1\rangle$ que pondremos en superposición con la puerta de Hadamard. Hadamard transforma a $|0\rangle$ en $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ y $|1\rangle$ en $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, por tanto,

$$|\varphi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] = \frac{|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle}{2} = \begin{bmatrix}+\frac{1}{2}\\-\frac{1}{2}\\+\frac{1}{2}\\-\frac{1}{2}\end{bmatrix} \tag{4.2}$$

Ahora, aplicaremos el oráculo U_f a la expresión $\frac{|0,0\rangle-|0,1\rangle+|1,0\rangle-|1,1\rangle}{2}$ y recordando que U_f no deja de ser una aplicación lineal. Por tanto, tenemos que

$$|\varphi_2\rangle = U_f\frac{|0,0\rangle - |0,1\rangle + |1,0\rangle - |1,1\rangle}{2} = \frac{U_f\,|0,0\rangle - U_f\,|0,1\rangle + U_f\,|1,0\rangle - U_f\,|1,1\rangle}{2} \tag{4.3}$$

Recordemos que nuestro oráculo U_f transforma $|x, y\rangle$ en $|x, y \oplus f(x)\rangle$, por lo que

$$|\varphi_2\rangle = \frac{|0, 0 \oplus f(0)\rangle - |0, 1 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |1, 1 \oplus f(1)\rangle}{2} = \frac{|0, f(0)\rangle - |0, \overline{f(0)}\rangle + |1, f(1)\rangle - |1, \overline{f(1)}\rangle}{2} \tag{4.4}$$

donde $\overline{f(x)}$ es el contrario de $f(x)$.

Recordemos que $|x, y\rangle$ no es más que una notación de $|x\rangle \otimes |y\rangle$, por tanto aplicando la propiedad distributiva del producto tensorial por la derecha tenemos

$$|\varphi_2\rangle = \frac{|0\rangle \otimes \left[|f(0)\rangle - |\overline{f(0)}\rangle\right] + |1\rangle \otimes \left[|f(1)\rangle - |\overline{f(1)}\rangle\right]}{2} \tag{4.5}$$

Observemos en un momento la expresión $|f(x)\rangle - |\overline{f(x)}\rangle$ para $x \in \{0, 1\}$ y discutimos su valor según el valor de $f(x)$.

$$|f(x)\rangle - |\overline{f(x)}\rangle = \begin{Bmatrix} |0\rangle - |1\rangle & \text{si} & f(x) = 0 \\ |1\rangle - |0\rangle & \text{si} & f(x) = 1 \end{Bmatrix} \tag{4.6}$$

que escribiremos como $(-1)^{f(x)}(|0\rangle - |1\rangle)$.

Aplicando esto a la expresión 4.5 tenemos que

$$|\varphi_2\rangle = \frac{(-1)^{f(0)}(|0\rangle \otimes [|0\rangle - |1\rangle]) + (-1)^{f(1)}(|1\rangle \otimes [|0\rangle - |1\rangle])}{2} \tag{4.7}$$

Hacemos uso de la propiedad distributiva por la derecha y reordenamos los escalares para separar la expresión en producto escalar de dos términos

$$|\varphi_2\rangle = \left[\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \tag{4.8}$$

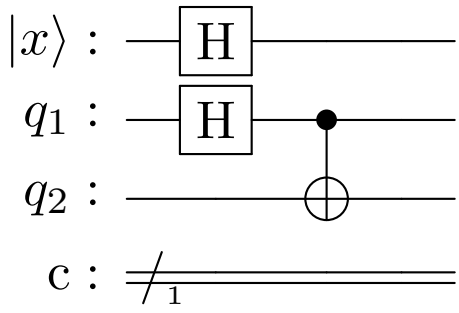
Discutamos el valor de la expresión $(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle$ según si $f(x)$ es constante o balanceada.

$$|\varphi_2\rangle = \begin{cases} (\pm 1)\left[\frac{|0\rangle+|1\rangle}{2}\right]\left[\frac{|0\rangle-|1\rangle}{2}\right] & \text{si } f \text{ es constante,} \\ (\pm 1)\left[\frac{|0\rangle-|1\rangle}{2}\right]\left[\frac{|0\rangle-|1\rangle}{2}\right] & \text{si } f \text{ es balanceada.} \end{cases} \tag{4.9}$$

Teniendo en cuenta que Hadamard es su propia inversa, llevará $\frac{|0\rangle+|1\rangle}{2}$ a $|0\rangle$ y $\frac{|0\rangle-|1\rangle}{2}$ a $|1\rangle$.

$$|\varphi_3\rangle = \begin{cases} (\pm 1)|0\rangle\left[\frac{|0\rangle-|1\rangle}{2}\right] & \text{si } f \text{ es constante,} \\ (\pm 1)|1\rangle\left[\frac{|0\rangle-|1\rangle}{2}\right] & \text{si } f \text{ es balanceada.} \end{cases} \tag{4.10}$$

Finalmente medimos el qubit superior para determinar si f es constante o balanceada, ya que si sale $|0\rangle$ será constante y si sale $|1\rangle$ será balanceada. Observamos que el signo no afecta a la proceso de medir, pues recordemos que la probabilidad de que sea un estado depende de la norma al cuadrado.



5. Conclusión

6. Bibliografía