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,* ***(Creo que está al revés, preguntar!!!)***

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

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

- *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 $|v\rangle\,|w\rangle$, $|vw\rangle$.*

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

$$\{|v_i\rangle \otimes |w_j\rangle \mid 1 \le i \le m, 1 \le j \le n\} \tag{2.27}$$

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

$$(f\otimes g)(|v\rangle \otimes |w\rangle) = f(|v\rangle) \otimes g(|w\rangle). \tag{2.28}$$

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:

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \dots & a_{1n}B \\ a_{21}B & a_{22}B & \dots & a_{2n}B \\ \vdots & \vdots & & \ddots \\ a_{m1}B & a_{m2}B & \dots & a_{mn}B \end{bmatrix} \vdots \tag{2.29}$$

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 $\mathbb{C}^n$.

3. Puertas Cuánticas

4. Algoritmos

4.1. ...

5. Conclusión

6. Bibliografía