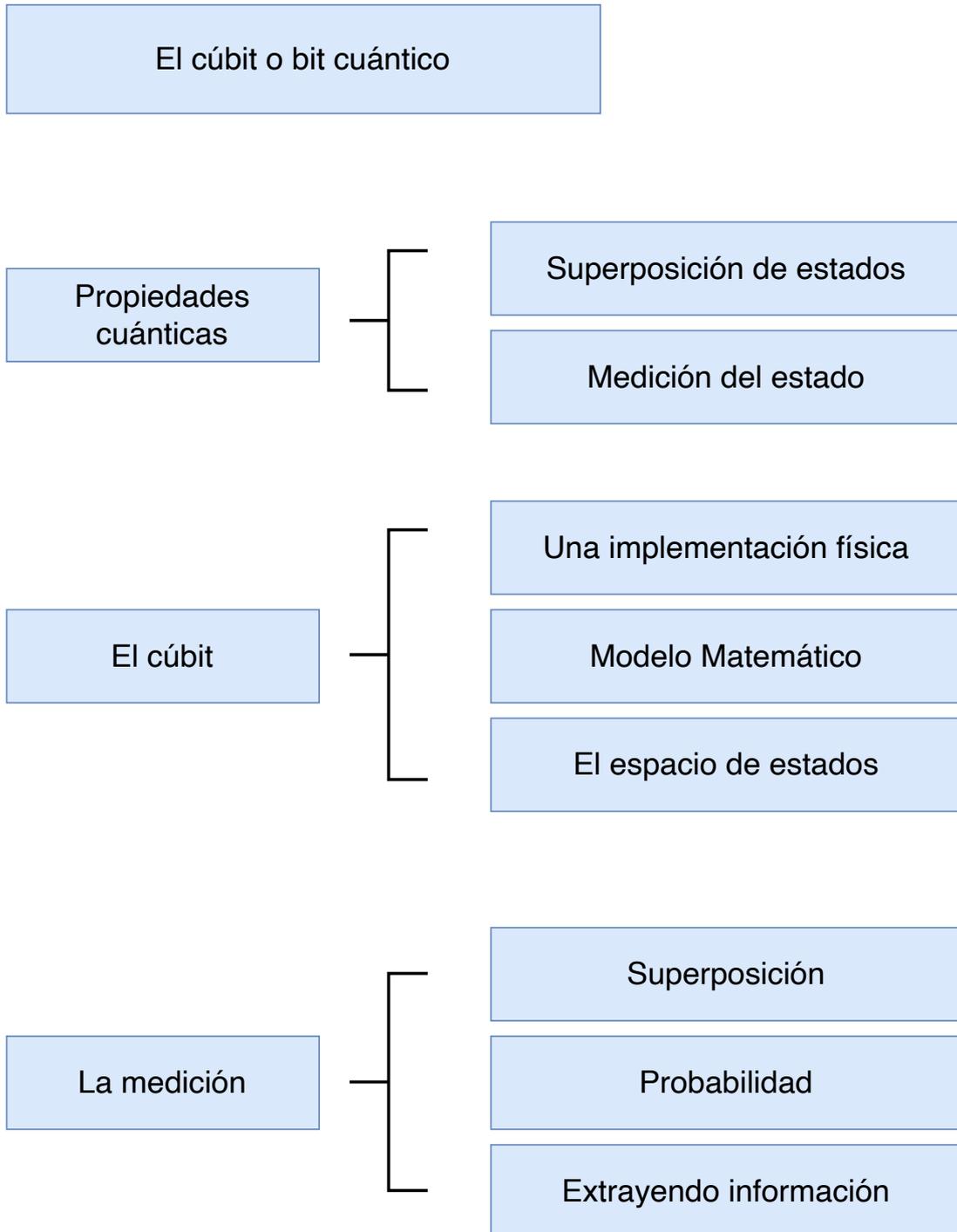


Computación Cuántica

Modelo de cúbit

Índice

Esquema.	2
Ideas clave	3
2.1 Introducción y objetivos	3
2.2 Las propiedades cuánticas	4
2.3 El bit cuántico o cúbit	9
2.4 La medición del cúbit	17
2.5 Puertas cuánticas	20
2.6 Referencias bibliográficas	27



2.1 Introducción y objetivos

De la misma forma que la unidad mínima de información y elemento fundamental en computación clásica es el bit, en computación cuántica, la unidad mínima de información e igualmente fundamental, es el bit cuántico o cúbit. La unidad mínima de procesamiento es el circuito cuántico que esta formado por una colección de bits cuánticos (un registro cuantico) y una serie de transformaciones aplicadas sobre ellos. La siguiente figura muestra un simple circuito cuántico de cuatro cúbits.

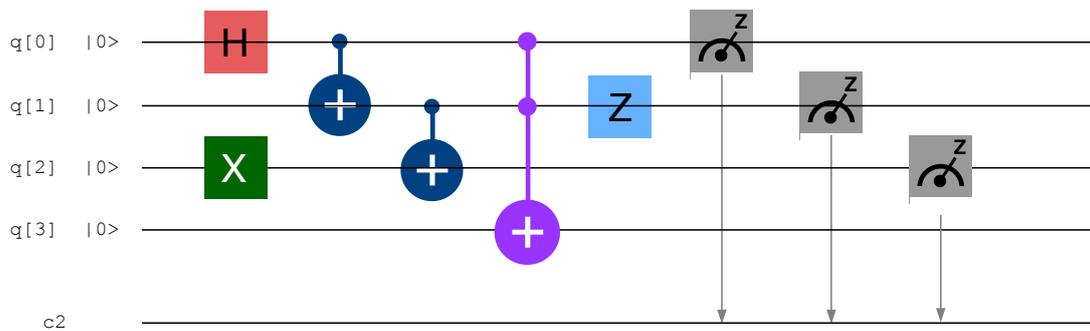


Figura 1: Ejemplo de circuito cuántico. Elaboración propia.

La implementación física de un bit clásico está basada en el transistor, ese componente de microelectrónica que hemos llegado a miniaturizar hasta la dimensión del nanómetro.

El transistor, actúa como un interruptor digital y es la base de los dispositivos electrónicos que nos rodean como ordenadores o teléfonos. Existen diferentes formas de implementar físicamente un bit clásico y de igual forma ocurre con el cúbit, se están explorando diferentes tecnologías de fabricación, como los cubits basados en circuitos superconductores, o en iones atrapados o con fotones, etc.

En computación clásica la implementación física del bit es algo totalmente abstrac-

to para el usuario y eso mismo ocurrirá también con el bit cuántico a medida que la industria madure, sin embargo en este momento, en los inicios de la computación cuántica comercial es todavía interesante conocer los fundamentos físicos de su implementación para entender sus propiedades y comportamiento. Con este objetivo se estudiará al principio de este tema una implementación física del cubit utilizando el fotón, la partícula elemental responsable de las manifestaciones cuánticas del fenómeno electromagnético.

A continuación se describen de forma precisa las propiedades fundamentales y el comportamiento de un cubit de forma abstracta, sin tener en cuenta ya su implementación física, finalmente se presenta la primera aplicación de la computación cuántica de la historia para la distribución de clave en criptografía. Finalmente se discute en detalle el espacio de estados del sistema cuántico formado por un cubit.

El objetivo de este tema es presentar el sistema cuántico más simple no trivial, un sistema con dos estados distinguibles, es decir el cúbit, una visión de su implementación con fotones, sus características, propiedades y comportamiento así como el espacio de estados en el que existe.

Los objetivos de este segundo tema de la asignatura son los siguientes:

- ▶ Las propiedades cuánticas
- ▶ El cúbit, la unidad mínima de información en computación cuántica
- ▶ El modelo de cúbit
- ▶ El espacio de estados
- ▶ El proceso de medición de un cúbit

2.2 Las propiedades cuánticas

Los sistemas cuánticos manifiestan un comportamiento que no resulta intuitivo comparado con el de nuestro mundo macroscópico, familiarizarnos con él es fundamental

para entender las propiedades del cubit y su comportamiento.

Para mostrar parte de estas propiedades realizaremos un experimento con luz y filtros polarizadores. Si dispones de un par de gafas polarizadas podrás comprobar su polarización mirando a través de ambas y girando una de ellas 90° con respecto de la otra. Si ambos pares de gafas están polarizados observaremos un oscurecimiento. Este oscurecimiento es debido a que la luz es una onda electromagnética que tiene campos eléctricos y magnéticos variables perpendiculares a la dirección en la que viaja, en este experimento consideraremos únicamente el campo eléctrico.

Para una fuente de luz, como la luz del sol, la luz está polarizada aleatoriamente, lo que significa que el vector eléctrico apunta en distintas direcciones. Un filtro polarizador impedirá el paso a todas las direcciones excepto aquella que coincide con el eje del filtro. Así, un filtro polarizador vertical, dejará pasar únicamente la dirección vertical del campo eléctrico y una vez la luz atraviesa el filtro diremos que está polarizada, en este caso, verticalmente.

La siguiente figura muestra el efecto en la intensidad de luz registrada en una pantalla al atravesar diferentes elementos.

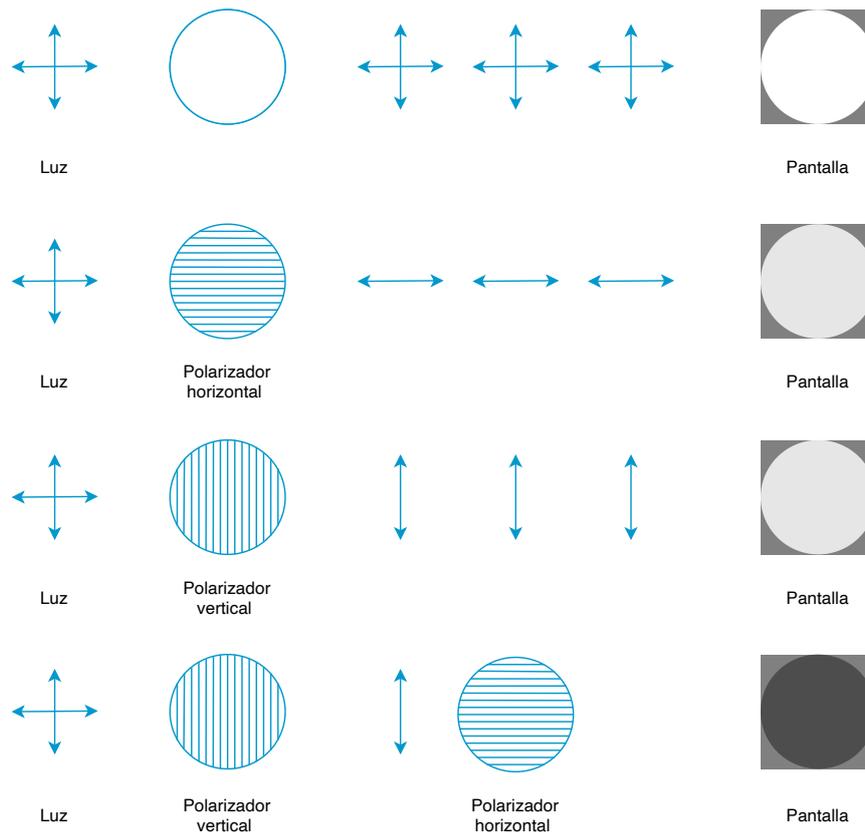


Figura 2: Efecto de distintas configuraciones de polarizadores sobre la intensidad de luz. Elaboración propia.

En el experimento veremos la relación entre la intensidad de la luz transmitida a través de los filtros polarizadores y el ángulo entre los ejes de los filtro.

Este simple experimento puede mostrar parte de las propiedades cuánticas del cúbit, que más adelante utilizaremos en computación, y entender el concepto de medida. Los formalismos de la mecánica cuántica que explican los resultados observados en este experimento proporcionan las bases para la descripción del cúbit.

Un filtro polarizador es un material que transmite, de forma selectiva, una determinada dirección de oscilación del campo eléctrico de una onda electromagnética (como la luz), bloqueando el resto de direcciones. La siguiente figura muestra un esquema de un filtro polarizador vertical, que solo deja pasar la componente vertical, otro horizontal y uno oblicuo a 45° .



Figura 3: Configuración incorporando un polarizador a 45° entre medias del polarizador vertical y horizontal. Elaboración propia.

Si tenemos una fuente de luz y una pantalla y entre ambas colocamos un filtro polarizador, por ejemplo horizontal, entonces observaremos que la intensidad de la luz en la pantalla disminuye, ya que solo llegan aquellos fotones con dirección horizontal. Si aplicamos un segundo filtro vertical, entre el filtro horizontal y la pantalla, entonces no se recibirá luz en la pantalla, ya que los fotones que habían superado el filtro anterior eran aquellos con dirección horizontal y no podrán, por tanto, atravesar el nuevo filtro vertical.

Si se agrega un tercer filtro entre los dos primeros, orientado en un ángulo de 45° , sorprendentemente, la luz llegará a la pantalla ¿por qué la presencia del tercer filtro, que debería servir solo para filtrar luz en la dirección de 45° , en realidad actúa permitiendo el paso de la luz?

A pesar de lo no intuitivo del resultado, es posible explicarlo mediante la mecánica ondulatoria clásica. Lo que ya no es posible de explicar de forma clásica es que el experimento se puede realizar, y muestra ese mismo comportamiento, cuando la fuente de luz es un solo fotón. En ese caso, solo la mecánica cuántica puede dar una explicación que consta de dos partes: un modelo del estado de polarización de un fotón y un modelo de la interacción entre el filtro polarizador y el fotón. La descripción de este experimento y la definición de un cúbit utilizan nociones básicas de álgebra lineal que se verá en otra de las asignaturas pero que repasaremos brevemente en las siguientes secciones. En mecánica cuántica se modela el estado de polarización de un fotón mediante un vector unitario, un vector de longitud 1. Utilizando la notación de Dirac, la notación estándar en mecánica cuántica para representar el estado cuántico, usaremos los siguientes kets para representar los vectores unitarios correspondientes a la polarización vertical y horizontal respectivamente:

$$|\uparrow\rangle \text{ y } |\rightarrow\rangle \quad (1)$$

Una polarización arbitraria se puede expresar como una combinación lineal de los vectores base anteriores:

$$|\Psi\rangle = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle \quad (2)$$

De esta forma el siguiente vector es unitario y representa la polarización a 45°:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}} |\uparrow\rangle + \frac{1}{\sqrt{2}} |\rightarrow\rangle \quad (3)$$

Los coeficientes α y β se denominan amplitudes de probabilidad de $|\Psi\rangle$ en las direcciones $|\uparrow\rangle$ y $|\rightarrow\rangle$ respectivamente. Cuando α y β son ambos distintos de cero, se dice que el estado está en superposición de $|\uparrow\rangle$ y $|\rightarrow\rangle$.

La mecánica cuántica modela la interacción entre un fotón y un filtro de polarización de la siguiente manera: el filtro tiene un eje de polarización, por ejemplo $|\uparrow\rangle$, cuando el fotón con polarización $|\nu\rangle = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle$ atraviesa el polarizador con eje de polarización $|\uparrow\rangle$, el fotón atravesará el polarizador con probabilidad $|\alpha|^2$ y será absorbido con probabilidad $|\beta|^2$, es decir, la probabilidad de que un fotón pase a través del filtro es el cuadrado de la magnitud de la amplitud de su polarización en la dirección del eje del polarizador. La probabilidad de que el fotón sea absorbido por el filtro es el cuadrado de la magnitud de la amplitud en la dirección perpendicular al eje del polarizador. Además, cualquier fotón que pase a través del filtro polarizador quedará polarizado en la dirección del eje del polarizador.

La naturaleza probabilística de la interacción y el cambio de estado resultante son características de todas las interacciones entre cúbit y dispositivos de medida, sin depender de su implementación física.

Un fotón polarizado horizontalmente no tiene amplitud en la dirección vertical, por lo que no tiene posibilidad de pasar a través del filtro vertical. Por esta razón, no llega luz a la pantalla. Si el polarizador vertical hubiera estado en cualquier otra dirección,

un fotón polarizado horizontalmente tendría cierta amplitud en la dirección del eje de polarización y algo de luz llegaría a la pantalla. Para comprender lo que sucede una vez que se inserta el tercer filtro, con el eje de polarización $|\nearrow\rangle$, expresaremos el estado de polarización del fotón polarizado horizontalmente de la siguiente forma:

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}} |\nearrow\rangle - \frac{1}{\sqrt{2}} |\nwarrow\rangle \quad (4)$$

Cualquier fotón que pase a través del polarizador horizontal se polariza horizontalmente, por lo que la amplitud del estado de dicho fotón en la dirección $|\nearrow\rangle$ será de $\frac{1}{\sqrt{2}}$.

Un fotón polarizado horizontalmente pasará a través del polarizador de 45° con probabilidad $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$. Cualquier fotón que haya pasado a través del polarizador a 45° tiene polarización $|\nearrow\rangle$. Cuando estos fotones alcanzan el tercer polarizador tienen amplitud en la dirección vertical, por lo que algunos de ellos (la mitad) atravesará el tercer polarizador, el polarizador con polarización vertical y llegarán a la pantalla. De esta manera, la mecánica cuántica explica cómo puede llegar más luz y cuánta luz llega a la pantalla cuando se agrega el tercer polarizador. En resumen, el estado de polarización de un fotón se modela como un vector unitario. Su interacción con un polarizador es probabilística y depende de la amplitud asociada a la componente de la polarización del fotón en la dirección del eje de polarización del polarizador, el fotón es absorbido, o el polarizador dejará el fotón con la polarización del polarizador.

2.3 El bit cuántico o cúbit

Podemos diseñar otro experimento con fotones para mostrar el concepto de superposición, para ello, empecemos por representar un bit clásico aprovechando la ubicación de un fotón.

En este experimento, utilizaremos los siguientes elementos:

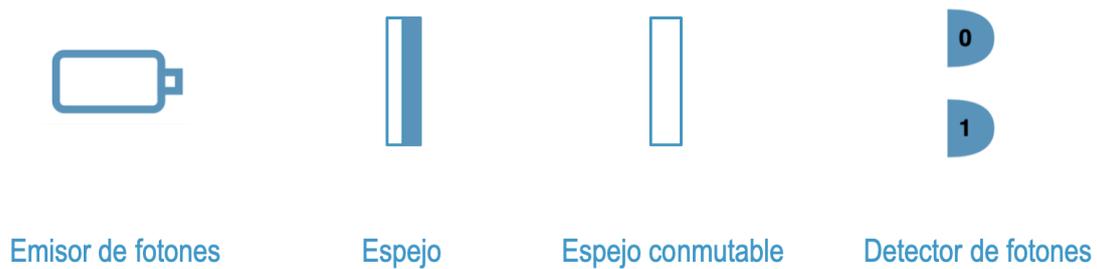


Figura 4: Elementos utilizados en los siguientes experimentos. Elaboración propia.

En la siguiente figura se muestra el experimento, que utiliza un espejo, un espejo conmutable, que puede reflejar la luz o ser transparente, un emisor de fotones y un detector. El espejo conmutable nos permite controlar el camino que seguirá el fotón para finalmente ser registrado por uno de los dos detectores, según el camino que haya seguido. En la siguiente figura se muestra la implementación física de un bit clásico de la forma descrita.

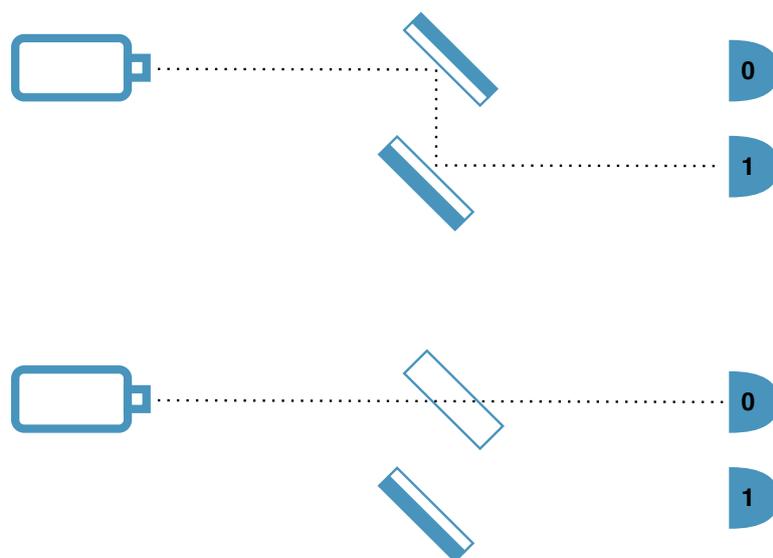


Figura 5: Implementación física de un bit clásico. Elaboración propia basada en la figura 2-1 del libro *Programming Quantum Computers*

Aprovechando esta instalación, podemos mostrar alguna de las propiedades del bit cuántico, para ello sustituimos el espejo conmutador por un espejo semiespejado, se trata de una superficie que puede dejar pasar la luz o reflejarla con igual probabilidad, dirigiendo la trayectoria del fotón hacia uno de los dos detectores.

Cuando un fotón alcanza la superficie del espejo semiespejado se produce un efecto

que no tiene equivalente clásico, ya que el fotón pasa a existir en un estado de superposición *de viajar* por cada uno de los dos caminos, el correspondiente al 0 y el correspondiente al 1. El bit ya no es clásico pues se encuentra en una superposición de 0 y 1. No sería correcto decir que el fotón se encuentra en ambos caminos al mismo tiempo pues solo existe un fotón indivisible y finalmente solo uno de los dos detectores registrara el fotón. Cuando se produce el registro del fotón en el detector, la superposición desaparece y el bit cuántico se convierte en un bit clásico proporcionando un resultado definido, 0 o 1.

El espacio de estados de polarización de un fotón es otro ejemplo de bit cuántico o cúbit. Un cúbit tiene infinitos estados posibles, cualquier estado representado por un vector unitario de la forma $a|\uparrow\rangle + b|\rightarrow\rangle$ se considera un estado válido del cúbit. Las amplitudes a y b son números complejos, aunque no necesariamente han de tener una parte imaginaria, como vimos en el caso de la polarización del fotón, pues en ese caso, los coeficientes imaginarios corresponden a la polarización circular. En general, el conjunto de todos los estados posibles de un sistema físico se denomina espacio de estados del sistema. Cualquier sistema cuántico que pueda modelarse mediante un espacio vectorial complejo de dimensión 2 puede tratarse como un cúbit. Estos sistemas los denominaremos sistemas cuánticos de dos estados y pueden ser, como hemos visto, la polarización de un fotón, el espín de un electrón, el estado fundamental y un estado excitado de un átomo, etc. El hecho de que denominemos a estos sistemas como sistemas de dos estados no significa que el espacio de estados tiene sólo dos estados, como hemos dicho, tiene infinitos, sino que todos los estados posibles pueden representarse como una combinación lineal, o superposición, de dos estados. Para que un espacio vectorial complejo bidimensional pueda tratarse como un cúbit, se deben distinguir dos estados linealmente independientes, como $|0\rangle$ y $|1\rangle$, $|\uparrow\rangle$ y $|\rightarrow\rangle$, $|+\rangle$ y $|-\rangle$, etc.. En teoría de la información cuántica y en computación cuántica, todos los sistemas de dos estados, ya sean de espín de electrones, de fotones o de niveles de energía de un átomo, son igualmente válidos. Desde un punto de vista de fabricación, todavía no está claro qué sistema de dos estados será óptimo para la implementación físicas de un procesador cuántico como tampoco lo era para el procesador clásico antes de la invención del transistor. La notación de Dirac o notación bra-ket es estándar en física cuántica para representar los estados cuánticos

y sus transformaciones. A continuación presentamos la parte de la notación de Dirac que se usa para los estados cuánticos. Es una notación fundamental para comprender todo el material posterior.

En la notación de Dirac, un ket como $|w\rangle$, donde w es una etiqueta arbitraria, se refiere a un vector que representa un estado de un sistema cuántico.

Un vector $|w\rangle$ es una combinación lineal de vectores $|s_1\rangle, |s_2\rangle, \dots, |s_n\rangle$ si existen números complejos a_i tales que $|w\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \dots + a_n|s_n\rangle$.

Un conjunto de vectores S , genera un espacio vectorial complejo V si cada vector $|v\rangle$ de V se puede escribir como una combinación lineal compleja de vectores en el conjunto, cada $|v\rangle \in V$ se puede escribir como: $|v\rangle = a_1|s_1\rangle + a_2|s_2\rangle + \dots + a_n|s_n\rangle$ para algunos $|s_i\rangle \in S$ y números complejos a_i .

Dado un conjunto de vectores S , el subespacio de todas las combinaciones lineales de vectores en S se denomina sistema generador(S). Un conjunto de vectores B para el cual cada elemento de V puede escribirse de forma única como una combinación lineal de vectores en B se denomina base de V . En un espacio vectorial bidimensional, dos vectores cualesquiera que no sean múltiplos entre sí forman una base. En mecánica cuántica, normalmente se requiere que las bases sean ortonormales, es decir ortogonales y normalizadas, así, los dos estados distinguibles, $|0\rangle$ y $|1\rangle$, deberán por tanto ser ortonormales.

Un producto escalar $\langle v_1|v_2\rangle$, o producto interno, en un espacio vectorial complejo V es una función compleja definida sobre pares de vectores $|v_1\rangle$ y $|v_2\rangle$ en V , que satisface las siguientes propiedades:

- $\langle v|v\rangle$ es real no negativo
- $\langle v_2|v_1\rangle = \langle v_1|v_2\rangle^*$
- $\langle a\langle v_2| + b\langle v_3||v_1\rangle = a\langle v_2|v_1\rangle + b\langle v_3|v_1\rangle$, donde \bar{z} es el complejo conjugado \bar{z}

$$z = a + ib.$$

$$\bar{z} = a - ib$$

Se dice que dos vectores $|v_1\rangle$ y $|v_2\rangle$ son ortogonales si $\langle v_1|v_2\rangle = 0$. Un conjunto de vectores es ortogonal si todos sus miembros son ortogonales entre sí.

La longitud, o norma, de un vector $|v\rangle$ es: $||v\rangle| = \sqrt{\langle v|v\rangle}$. Dado que todos los vectores $|x\rangle$ que representan estados cuánticos son de longitud unitaria, $\langle x|x\rangle = 1$ para cualquier vector de estado $|x\rangle$.

Se dice que un conjunto de vectores es orto-normal si todos sus elementos son de longitud uno y ortogonales entre sí: un conjunto de vectores $B = |\beta_1\rangle, |\beta_2\rangle, \dots, |\beta_n\rangle$ es orto-normal si $\langle \beta_i|\beta_j\rangle = \delta_{ij} \forall i, j$, donde:

$$\delta_{ij} = 1(i = j)$$

$$\delta_{ij} = 0(i \neq j)$$

En mecánica cuántica interesan principalmente las bases orto-normales, por lo que siempre que se haga referencia a una base se tratará de una base orto-normal a menos que se indique lo contrario.

Para que el espacio de estados de un sistema de dos estados represente un bit cuántico, se deberán especificar dos estados distinguibles orto-normales, etiquetados como $|0\rangle$ y $|1\rangle$. Los estados pueden ser elegidos arbitrariamente siempre y cuando estos sean orto-normales. Por ejemplo, en el caso de la polarización de fotones, podemos elegir $|0\rangle$ y $|1\rangle$ para que correspondan con los estados $|\uparrow\rangle$ y $|\rightarrow\rangle$, o $|\nearrow\rangle$ y $|\searrow\rangle$. Seguiremos la convención de asignar $|0\rangle = |\uparrow\rangle$ y $|1\rangle = |\rightarrow\rangle$, lo que implica que $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ y $|\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. En el caso del espín del electrón, $|0\rangle$ y $|1\rangle$ podrían corresponder a espín hacia arriba y espín hacia bajo respectivamente, o espín a la izquierda y espín a la derecha.

Al hablar de cúbits, de computación cuántica o de teoría cuántica de la información, se debe fijar una base estándar $|0\rangle, |1\rangle$ y, por coherencia, se deberá mantener fija durante todo el discurso.

En computación cuántica, los valores clásicos del bit 0 y 1 se codifican como los estados distinguibles $|0\rangle$ y $|1\rangle$. Esta codificación permite una comparación directa entre bits y cúbits: los bits pueden tomar solo dos valores, 0 y 1, mientras que los cúbits

pueden tomar no solo los valores $|0\rangle$ y $|1\rangle$ sino también cualquier superposición de estos valores, $a|0\rangle + b|1\rangle$, donde a y b son números complejos tales que la suma de sus cuadrado de sus módulos es la unidad

$$|a|^2 + |b|^2 = 1$$

Tanto los vectores, que representan los estados, como las matrices, que representan las transformaciones lineales, se pueden escribir utilizando la notación matricial una vez que la base ha sido establecida.

De ese modo, si se ha establecido la base $B = |\beta_1\rangle, |\beta_2\rangle$ entonces, el ket $|v\rangle = a|\beta_1\rangle + b|\beta_2\rangle$ puede representarse como:

$$\begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}$$

El ket $|v\rangle$ corresponde a un vector columna v , donde v es una etiqueta, el nombre del vector.

El traspuesto conjugado v^\dagger de un vector:

$$v = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}; v^\dagger = (\bar{\beta}_1 \quad \bar{\beta}_2)$$

En notación de Dirac, el traspuesto conjugado de un ket se denomina bra, que corresponde a un vector columna v^\dagger , y se escribe como: $\langle v|$

$$|v\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}; \langle v| = (\bar{\beta}_1 \quad \bar{\beta}_2)$$

Dados dos vectores de coeficientes complejos:

$$|\alpha\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} \text{ y } |\beta\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix}$$

el producto escalar $\langle\alpha|\beta\rangle$, o braket, se define como el escalar resultado de multiplicar el traspuesto conjugado de $\langle\alpha| = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$ por $|\beta\rangle$

$$\langle \alpha | \beta \rangle = \langle \alpha | | \beta \rangle = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n) \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_n \end{pmatrix} = \sum_{i=1}^n \bar{\alpha}_i \beta_i$$

Dado que $|0\rangle$ y $|1\rangle$ son ortogonales y están normalizados, se deberán cumplir las siguientes igualdades:

$$v = a|0\rangle + b|1\rangle$$

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

$$\langle 1|1\rangle = 1$$

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

$$\langle 0|v\rangle = a$$

$$\langle 1|v\rangle = b$$

Fijando la base estándar, también denominada base computacional, como: $\{|0\rangle, |1\rangle\}$ y en ese orden, los vectores de la base $|0\rangle$ y $|1\rangle$ se pueden expresar como:

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

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

y de esta forma, una combinación lineal genérica $|v\rangle = a|0\rangle + b|1\rangle$ se representa como:

$$|v\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

Esta elección de la base así como del orden de los vectores que forman la base es arbitraria. La siguiente representación sería igualmente válida siempre y cuando se mantenga la consistencia:

$$|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

$$|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

A menos que se informe de lo contrario, todos los vectores y matrices se escribirán utilizando como referencia la base estándar o base computacional $\{|0\rangle, |1\rangle\}$ y en ese orden.

Un estado cuántico $|v\rangle$ es una superposición de los vectores de la base $\{|\beta_1\rangle, |\beta_2\rangle\}$, si es una combinación lineal no trivial de $|\beta_1\rangle$ y $|\beta_2\rangle$, si $|v\rangle = a_1|\beta_1\rangle + a_2|\beta_2\rangle$ siendo a_1 y a_2 distintos de cero.

Para que el término superposición tenga sentido deberá referirse a una base. Cuando se mencione el término “superposición” sin especificar explícitamente la base, este se referirá a la base estándar o base computacional.

Utilizando el entorno de desarrollo de QISKit, realiza el siguiente experimento.

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

```
# Importar las librerías de QISKit necesarias para el experimento

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 inicialización al cúbit
```

```
qc.initialize(ket, 0)

# Visualizar el circuito

qc.draw()
```

La notación matricial es más conveniente para realizar cálculos, pero siempre requiere la elección de una base y un orden de vectores dentro de la base. La notación de Dirac o braket tiene la ventaja de ser independiente de la base y del orden de los elementos básicos. También es más compacta e intuitiva, al sugerir relaciones correctas entre los elementos, como hemos visto en el caso del producto escalar, por lo que una vez que se hace familiar, es más fácil y rápida de usar.

En lugar de cúbits, los sistemas físicos con estados modelados por espacios vectoriales de dimensión superior a 2 podrían también usarse como unidades básicas de información y computación. Las unidades de información que utilizan tres estados distinguibles se denominan qutrits y las unidades de n valores se denominan qudits. Dado que los qudits se pueden modelar utilizando múltiples cúbits, un modelo de información cuántica basado en qudits tiene el mismo poder computacional que uno basado en cúbits. Por esta razón, no se consideran más los qudits, al igual que en la computación clásica se usa el modelo binario basado en bits.

Hasta el momento tenemos un modelo matemático con el que describir los bits cuánticos pero todavía no tenemos un modelo matemático para realizar las medidas de los dispositivos físicos, los procesadores cuánticos y su interacción con los cúbits, los bits cuánticos.

2.4 La medición del cúbit

La interacción entre un fotón y un filtro de polarización, muestra las propiedades fundamentales de la interacción entre un dispositivo de medición y un sistema cuántico.

El modelo matemático utilizado para la descripción del experimento podemos extenderlo para la medición de cualquier cúbit individual, cualquiera sea su implementación física. El proceso de medida de un sistema cuántico más complejo, conserva las características de la medición de un solo cúbit como la naturaleza probabilística de los resultados o el efecto que el proceso de medida tiene sobre el estado del sistema. En este apartado, estudiaremos la medida de sistemas cuánticos formados por un único cúbit, dejando para más adelante la medida de un sistema cuántico general. La teoría cuántica postula que cualquier dispositivo que mida un sistema cuántico de dos estados debe tener dos estados distinguibles cuyos vectores representativos, $|u\rangle$, $|u_{\perp}\rangle$, forman una base orto-normal para el espacio vectorial asociado. La medición de un estado transforma el estado en uno de los vectores de la base asociados al dispositivo de medida. La probabilidad de que el resultado de la medida del estado sea el vector base $|u\rangle$ es el cuadrado de la magnitud de la amplitud del componente del estado en la dirección del vector base $|u\rangle$. Por ejemplo, dado un dispositivo para medir la polarización del fotón, con una base asociada $|u\rangle$, $|u_{\perp}\rangle$, la probabilidad de que el resultado de la medida del estado $|v\rangle = a|u\rangle + b|u_{\perp}\rangle$ sea $|u\rangle$ será de $|a|^2$ y la probabilidad asociada a $|u_{\perp}\rangle$ será $|b|^2$.

Este comportamiento en la medición es un postulado de la mecánica cuántica, es una evidencia que no es susceptible de demostración, no se deriva de otros principios físicos sino de la observación empírica de experimentos con dispositivos de medida. Si la mecánica cuántica es correcta, todos los dispositivos que miden cúbits individuales deben comportarse de esta manera; todos tienen bases asociadas y el resultado de la medición es siempre uno de los dos vectores base, es por ello, que al realizar una medida de un cubito siempre se debe especificar la base con respecto a la cual se realizará la medición. Por defecto, y a no ser que se especifique lo contrario, las mediciones se realizarán con respecto a la base estándar o base computacional $\{|0\rangle, |1\rangle\}$.

El proceso de medida del sistema cuántico modifica su estado, si el sistema se encuentra en un estado $|v\rangle = a|u\rangle + b|u_{\perp}\rangle$ y el resultado de la medida resulta $|u\rangle$, entonces el estado del sistema deja de ser $|v\rangle$ y pasa a ser $|u\rangle$. Una segunda medición con respecto a la misma base devolverá $|u\rangle$ con probabilidad 1, es decir, tendremos la certeza de medir $|u\rangle$. A menos que el estado del sistema sea uno de los estados base, en cuyo

caso el estado inicial y el estado tras la medida coincidirían, la medición modificará el estado de forma irreversible haciendo imposible determinar el estado inicial antes de realizar cualquier medición.

Si bien el modelo matemático que describe la medición del cúbit en estado de superposición $a|0\rangle + b|1\rangle$ con respecto a la base computacional es claro, el proceso de medida plantea preguntas sobre el significado de la superposición. El concepto de superposición está asociado a la base, cualquier estado es una superposición con respecto a una base pero no con respecto a otras. Por ejemplo, el estado $a|0\rangle + b|1\rangle$ es una superposición con respecto a la base $\{|0\rangle, |1\rangle\}$ pero no con respecto a la base $a|0\rangle + b|1\rangle, b|0\rangle - a|1\rangle$. Por otro lado, y debido a la naturaleza probabilística del resultado de la medida, podría resultar tentador pensar en el estado $|\nu\rangle = a|0\rangle + b|1\rangle$ como una mezcla probabilística de $|0\rangle$ y $|1\rangle$, pero no lo es, no es cierto que el estado sea realmente $|0\rangle$ y $|1\rangle$ y que simplemente no sepamos cuál sino que $|\nu\rangle$ es un estado definido, que al ser medido con respecto a ciertas bases, da resultados deterministas, mientras que con respecto a otras, proporciona resultados aleatorios: un fotón cuyo estado de polarización es $|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle)$ se comporta determinísticamente cuando se mide con respecto a la base de Hadamard $|\nearrow\rangle, |\searrow\rangle$, pero proporciona resultados aleatorios cuando se miden con respecto a la base estándar $|\uparrow\rangle, |\rightarrow\rangle$.

Siempre que no se tome de forma literal, se puede pensar en la superposición como un estado en el que el cúbit está en el estado $|0\rangle$ y en el estado $|1\rangle$ al mismo tiempo pues estados en superposición uniforme de $|0\rangle$ y $|1\rangle$, es decir, que tienen la misma probabilidad pero con amplitudes diferentes, como $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ o $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, representan estados diferentes. Dado que un cúbit puede encontrarse en cualquiera de los infinitos estados posibles, se podría esperar que un solo cúbit pudiera almacenar mucha información clásica. Sin embargo, como hemos visto, las propiedades del proceso de medida limitan la cantidad de información que se puede extraer de un cúbit. La información almacenada en el cúbit se puede obtener solo mediante la medición, y cualquier medición da como resultado uno de dos estados, los dos estados correspondientes a la base asociada con el dispositivo de medición, por lo tanto, una sola medida produce como máximo un solo bit clásico de información y ya que la medida cambia el estado, no se pueden realizar dos mediciones del

estado original del cúbit. Además, como veremos, el teorema de no clonado impide la clonación de un estado cuántico desconocido, lo que nos conduce de nuevo a la imposibilidad de realizar dos medidas del estado del cúbit, ni siquiera indirectamente copiando el estado del cúbit y midiendo la copia y por ello, aunque existen infinitos estados de superposición del cúbit, solamente se puede extraer de él un bit clásico de información.

2.5 Puertas cuánticas

Utilizando el entorno de desarrollo de QISKit Quantum Lab, implementación de las principales puertas cuánticas.

Ejemplo 2. Puertas cuanticas

```
# Importar librerías de QISKit

from qiskit import QuantumRegister, ClassicalRegister

from qiskit import QuantumCircuit

from qiskit import IBMQ, Aer, execute

import numpy as np

from qiskit_textbook.tools import array_to_latex

# -----

# Puerta X (Pauli X o bit-flip)

# Rotación de  $\pi$  con respecto al eje X.

# Equivalente cuántico de la puerta NOT clásica.

# Asigna:
```

```

# |0>->|1>

# |1>->|0>

X = [[0,1],[1,0]]

array_to_latex(X, pretext = "\\text{Puerta X} = ", precision=1)


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


q = QuantumRegister(1)

qc = QuantumCircuit(q)

qc.x(q[0]) qc.draw()

```



```

# -----

# Puerta Z (Pauli Z o Phase shift)

# Rotación de  $\pi$  con respecto al eje Z.

# No actua sobre el estado |0>

# Asigna:

# |0>->|1>

# |1>->|0>

Z = [[1,0],[0,-1]]

array_to_latex(Z, pretext = "\\text{Puerta Z} = ", precision=1)


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


```

```
q = QuantumRegister(1)
```

```
qc = QuantumCircuit(q)
```

```
qc.z(q[0]) qc.draw()
```



```
# -----
```

```
# Puerta H (Hadamard)
```

```
# Rotación de  $\pi$  respecto eje X +  $\pi/2$  respecto eje Z
```

```
# Transforma el estado  $|0\rangle$  en la superposición uniforme
```

```
# Asigna:
```

```
#  $|0\rangle \rightarrow (|0\rangle + |1\rangle) / \sqrt{2}$ 
```

```
#  $|1\rangle \rightarrow (|0\rangle - |1\rangle) / \sqrt{2}$ 
```

```
H = [[1,1],[1,-1]]/np.sqrt(2)
```

```
array_to_latex(H, pretext = "\\text{Puerta H} = ", precision=1)
```

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

```
q = QuantumRegister(1)
```

```
qc = QuantumCircuit(q)
```

```
qc.h(q[0]) qc.draw()
```



```

# -----

# Puerta S (Fase)

# Rotación de  $\pi/2$  respecto eje Z

# Transforma el estado  $|1\rangle$  en  $i|1\rangle$ 

# Asigna:

#  $|0\rangle \rightarrow |0\rangle$ 

#  $|1\rangle \rightarrow i|1\rangle$ 

S = [[1,0],[0,i]]

array_to_latex(S, pretext = "\\text{Puerta S} = ", precision=1)

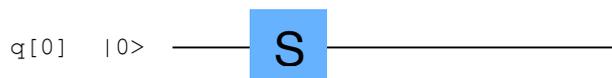

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$


q = QuantumRegister(1)

qc = QuantumCircuit(q)

qc.s(q[0]) qc.draw()

```



```

# -----

# Puerta CNOT (Controlled NOT)

# Puerta de dos cúbits (control y target)

# Si el cubit de control (superior en el ejemplo) vale  $|1\rangle$ 

# entonces la puerta NOT actúa sobre el cúbit target

# Asigna:

```

```

# |00>->|00>

# |01>->|11>

# |10>->|10>

# |11>->|11>

CX = [[1,0,0,0],[0,0,0,1],[0,0,1,0],[0,1,0,0]]

array_to_latex(CX, pretext = "\\text{Puerta CNOT} = ", precision=1)

```

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

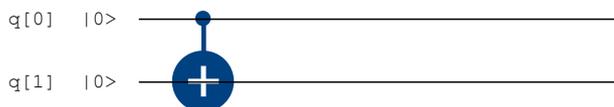
```

q = QuantumRegister(2)

qc = QuantumCircuit(q)

qc.cx(q[0],q[1]) qc.draw()

```



```

# -----

# Puerta CZ (Controlled Z)

# Puerta de dos cúbits (control y target)

# Si el cubit de control (superior en el ejemplo) vale |1>

# entonces la puerta Z actúa sobre el cúbit target

# Asigna:

# |00>->|00>

```

```
# |01>->|01>

# |10>->|10>

# |11>->-|11>

CZ = [[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,-1]]

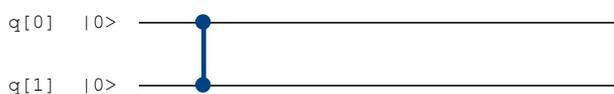
array_to_latex(CZ, pretext = "\\text{Puerta CZ} = ", precision=1)
```

$$CZ = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$$

```
q = QuantumRegister(2)

qc = QuantumCircuit(q)

qc.cz(q[0],q[1]) qc.draw()
```



```
# -----

# Puerta CCNOT (Controlled Controlled NOT o Toffoli)

# Puerta de tres cúbits (dos de control y target)

# Si los cubits de control valen |1>entonces

# la puerta NOT actúa sobre el cúbit target

# Asigna:

# |000>->|000>

# |001>->|001>
```

```

# |010>->|010>
# |011>->|111>
# |100>->|100>
# |101>->|101>
# |110>->|110>
# |111>->|011>

```

```
CCX = [[1,0,0,0,0,0,0,0],
```

```
[0,1,0,0,0,0,0,0],
```

```
[0,0,1,0,0,0,0,0],
```

```
[0,0,0,0,0,0,0,1],
```

```
[0,0,0,0,1,0,0,0],
```

```
[0,0,0,0,0,1,0,0],
```

```
[0,0,0,0,0,0,1,0],
```

```
[0,0,0,1,0,0,0,0]]
```

```
array_to_latex(CCX, pretext = "\\text{Puerta CCX} = ", precision=1)
```

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

```
q = QuantumRegister(3)
```

```
qc = QuantumCircuit(q)
```

```
qc.ccx(q[0],q[1],q[2])
```

```
qc.draw()
```



2.6 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