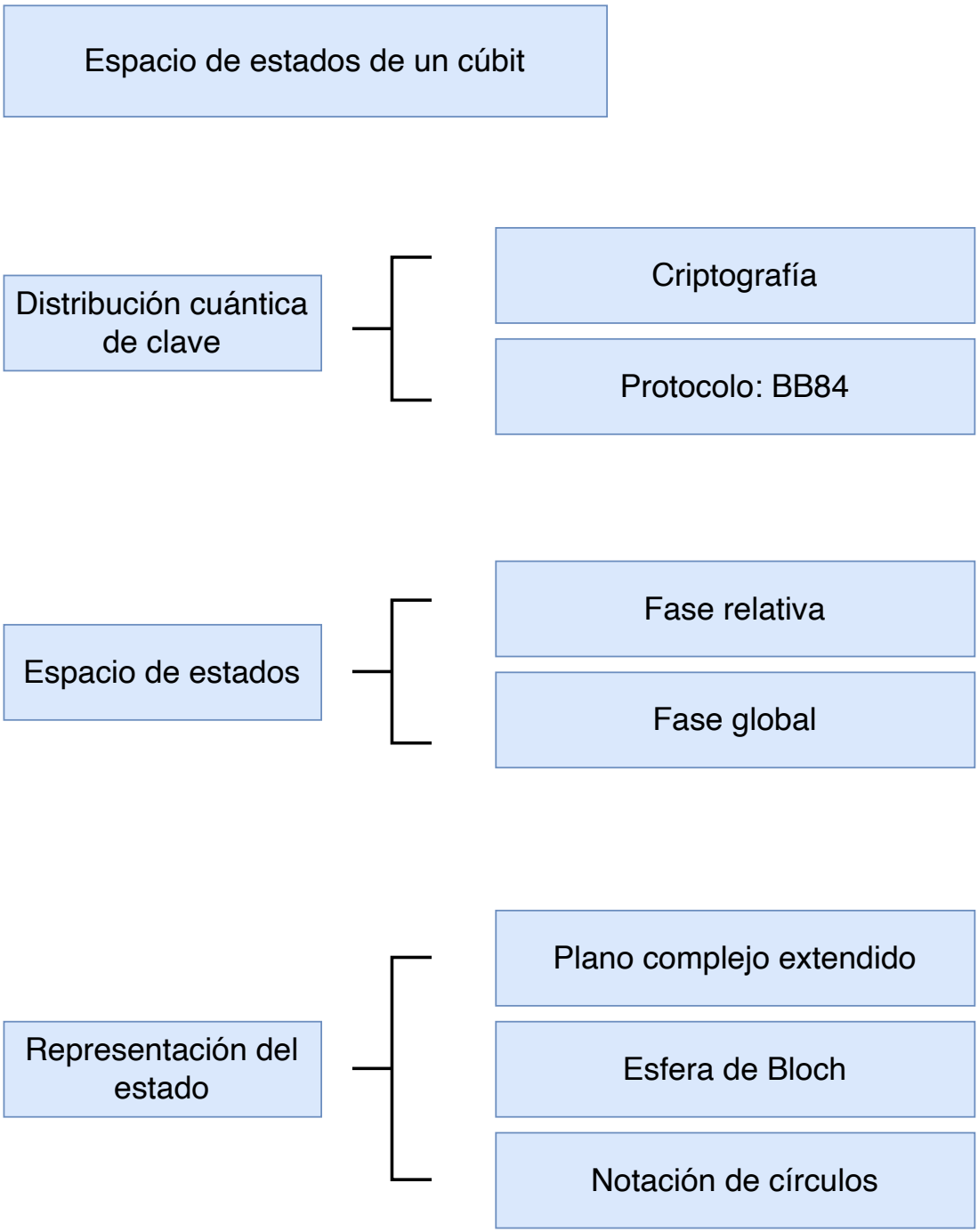
Computación Cuántica

El espacio de estados de un bit cuántico

Índice

Esquema


Espacio de estados de un cúbit
Distribución cuántica de clave
Criptografía
Protocolo: BB84
Espacio de estados
Fase relativa
Fase global
Representación del estado
Plano complejo extendido
Esfera de Bloch
Notación de círculos

Ideas clave

3.1 Introducción y objetivos

La introducción a la teoría cuántica presentada en los temas anteriores permite describir una primera aplicación del procesamiento de información cuántica a la seguridad de las comunicaciones: la distribución cuántica de claves.

> *La medición no es un proceso pasivo como se suponía en la mecánica clásica, ya que altera al sistema.*

La distribución cuántica de claves es un protocolo que no tiene un equivalente clásico y que permite generar una clave secreta aleatoria (no pseudo-aleatoria, sino genuinamente aleatoria aprovechando las leyes de la mecánica cuántica) y compartida entre dos partes, que usarán posteriormente para cifrar y descifrar mensajes.

A continuación se profundiza en el espacio de estados de un sistema de un cúbit, los conceptos de fase relativa y fase global. SI bien el estado cuántico no es observable, el uso de simuladores nos permite acceder a él, en la sección correspondiente a Visualización del estado de un bit cuántico se muestran diferentes opciones de representación del estado cuántico de un cúbit.

- Una aplicación de la computación cuántica: QKD
- Espacio de estados de un bit cuántico
  - Fase relativa
  - Fase global
- Visualización del estado
  - Plano complejo extendido

- Esfera de Bloch
- Notación con círculos

3.2 Aplicación: QKD, la distribución cuántica de claves

La criptografía trata la transmisión y almacenamiento de datos de manera que no puedan ser comprendidos ni modificados por terceros, los protocolos de criptografía utilizados actualmente necesitan que las dos partes que se quieren comunicar intercambien de forma segura una o más claves que utilizaran para el cifrado, siendo por tanto el intercambio y transmisión de las claves el punto más débil de todo el proceso.

Existen dos tipos principales de criptografía: criptografía simétrica y criptográfica asimétrica. La criptografía simétrica utiliza una única clave (previamente compartida entre el emisor y el receptor) para cifrar y descifrar el mensaje. La criptografía asimétrica se basa en el uso de dos claves: una clave pública que se puede difundir a todos aquellos que quieran cifrar el mensaje y una clave privada que no debe revelarse nunca. Si el emisor quiere enviar un mensaje cifrado solo tendrá que cifrarlo con la clave pública del receptor, que está asociada a la privada, y que solo el receptor podrá descifrar aplicando la clave privada. Tanto la criptografía simétrica como la asimétrica se utilizan ampliamente, a menudo de forma combinada, en multitud de aplicaciones, como la seguridad de Internet, las compras online, el correo electrónico, etc.

Los protocolos de distribución de claves cuánticas establecen una clave simétrica entre dos partes, Alice y Bob.

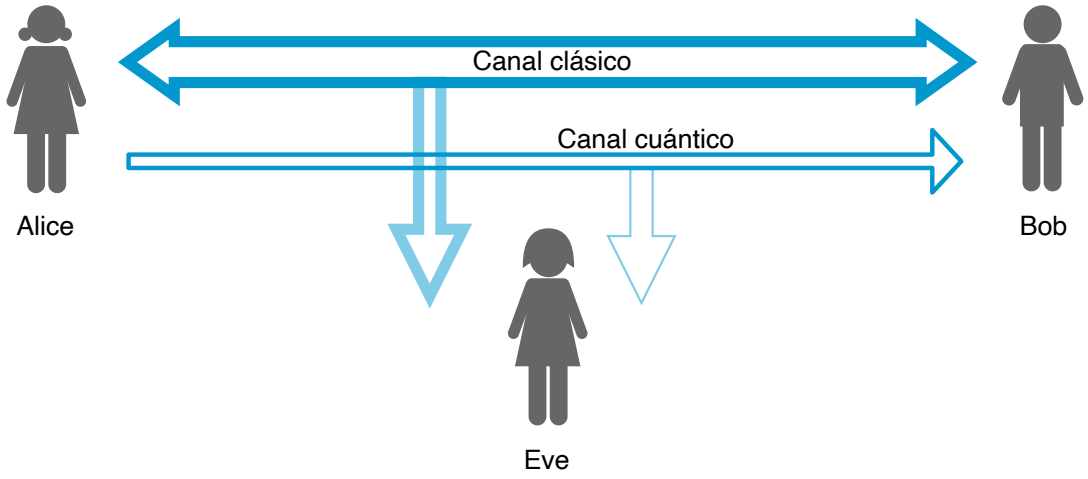


Figura 1: Actores y canales presentes en la distribución cuántica de clave. Elaboración propia.

En general, los protocolos de distribución cuántica de claves se pueden utilizar para reemplazar los protocolos clásicos, sin embargo, a diferencia de la distribución clásica, la seguridad de la distribución cuántica se basa en las propiedades fundamentales de la mecánica cuántica, mientras que los protocolos clásicos se basan en la dificultad computacional de un determinado problema. El primer protocolo de distribución de claves cuánticas se conoce como BB84 por sus inventores, Charles Bennett y Gilles Brassard, y 1984, el año en el que fue publicado. El objetivo del protocolo BB84 es establecer una clave secreta, una secuencia aleatoria de valores de bits 0 y 1, conocida solo por las dos partes, Alice y Bob, quienes pueden usar esta clave para tareas criptográficas como la de intercambiar mensajes secretos o la detección del intento de manipulación por un tercero, Eve.

El protocolo BB84 permite a Alice y Bob estar seguros de que si no detectan problemas al intentar establecer una clave, es muy probable que sea secreta. Sin embargo, el protocolo no garantiza que logren establecer una clave privada. Suponga que Alice y Bob están conectados por dos canales públicos: un canal clásico bidireccional ordinario y un canal cuántico unidireccional. El canal cuántico permite a Alice enviar una secuencia de cúbits (implementados como fotones individuales) a Bob, cada fotón será un cúbit. La información estará codificada como estados de polarización de los fotones. Ambos canales pueden ser observados por una espía, que llamaremos Eve.

Para comenzar el proceso de establecer una clave privada, Alice generar una secuen-

cia aleatoria de bits clásicos. A continuación Alice codifica aleatoriamente cada bit de esta secuencia en el estado de polarización de un fotón eligiendo aleatoriamente para cada bit una de las siguientes dos bases acordadas para codificarlo: la base estándar, polarización vertical u horizontal:

$0 \rightarrow |\uparrow>$

$1 \rightarrow |\rightarrow>$,

o la base de Hadamard, polarización *diagonal*:

$0 \rightarrow |\nearrow> = \frac{1}{\sqrt{2}}(|\uparrow> + |\rightarrow>)$,

$1 \rightarrow |\nwarrow> = \frac{1}{\sqrt{2}}(|\uparrow> - |\rightarrow>)$

Alice envía esta secuencia de fotones a Bob a través del canal cuántico. Bob mide el estado de cada fotón que recibe eligiendo cualquiera de las bases al azar. A través del canal clásico, Alice y Bob comprueban que Bob ha recibido un fotón por cada uno que Alice ha enviado, y solo entonces Alice y Bob comparten las bases que utilizaron para codificar y decodificar (medir) cada cúbit. Cuando la elección de las bases coincide, el valor de bit medido de Bob coincide con el valor de bit que envió Alice. Cuando eligieron diferentes bases, la probabilidad de que el bit de Bob coincida con el de Alice es solo del 50 %. Sin revelar los valores de los bits en sí mismos, que también Eve podría leer, no hay forma de que Alice y Bob averigüen cuáles de estos valores de bits están de acuerdo y cuáles no, de forma que descartan todos los bits en los que la elección de bases no coinciden, un promedio del 50 % se descartarán.

Luego, dependiendo del nivel de seguridad que requieran, Alice y Bob comparan un cierto número de valores de bits para comprobar que no se ha producido ninguna escucha. Estos bits también se descartarán y solo los bits restantes se utilizarán como clave privada.

A continuación se describe un tipo de ataque que puede realizar Eve y cómo los aspectos cuánticos de este protocolo impiden que el ataque tenga éxito.

Alice y Bob utilizan el canal clásico solo para la elección de las bases y no para los valores de los bits, por lo que Eve no puede obtener ninguna información sobre la clave

escuchando solo el canal clásico. Para obtener información, Eve debe interceptar los fotones transmitidos por Alice a través del canal cuántico. Eve debe enviar fotones a Bob antes de saber la elección de bases que hicieron Alice y Bob, ya que ellos compararán las bases solo después de que Bob haya confirmado la recepción de los fotones. Si envía diferentes fotones a Bob, Alice y Bob detectarán que algo anda mal cuando comparan los valores de los bits, pero si envía los fotones originales a Bob sin hacer nada, no obtiene información. Para obtener información, Eve deberá realizar una medición antes de enviar los fotones a Bob, para ello, en lugar de usar un polarizador para medir, Eve puede usar un cristal de calcita y un detector de fotones; un haz de luz que lo atraviesa se divide en dos haces separados espacialmente, uno polarizado en la dirección del eje óptico del cristal y el otro polarizado en la dirección perpendicular al eje óptico. Un detector de fotones colocado en uno de los haces realiza una medición cuántica. Dado que Alice aún no le ha dicho a Bob su secuencia de bases, Eve no sabe en qué base medir cada bit. Si mide los bits al azar, medirá utilizando la base incorrecta aproximadamente la mitad del tiempo. Cuando usa la base incorrecta para medir, la medición cambia la polarización del fotón antes de que se reenvíe a Bob. Este cambio en la polarización significa que, incluso si Bob mide el fotón en la misma base que Alice usó para codificar el bit, obtendrá el valor de bit correcto solo la mitad del tiempo.

En general, para cada uno de los cubits que retienen Alice y Bob, si Eve midió el qubit antes de enviarlo a Bob, habrá un 25 por ciento de posibilidades de que Bob mida un valor de bit diferente al que envió Alice. Por lo tanto, este ataque al canal cuántico está destinado a introducir una alta tasa de error que Alice y Bob detectan al comparar un número suficiente de bits en el canal clásico. Si estos bits coinciden, los bits restantes pueden utilizarse como clave privada.

Por lo tanto, no solo es probable que la versión de la clave de Eve sea incorrecta, sino que Alice y Bob pueden detectar el hecho de que alguien está escuchando y corren poco riesgo de establecer una clave comprometida; o logran crear una clave privada o detectan que se ha producido una escucha.

Eve no sabe en qué base medir los cubits, una propiedad crucial para la seguridad de este protocolo, porque Alice y Bob comparten información sobre qué bases usaron

sólo después de que Bob haya recibido los fotones; si Eve supiera en qué base medir los fotones, sus mediciones no cambiarían el estado y podría obtener los valores de los bits sin que Bob y Alice se dieran cuenta de nada sospechoso.

Una forma aparentemente fácil para que Eve supere este obstáculo es que ella copie el cúbit, quedándose con una copia para ella mientras envía el original a Bob, después de conocer la base correcta al escuchar el canal clásico podría leer su copia. Pero de nuevo, este ataque fracasaría gracias a una propiedad de la información cuántica: el principio de no clonado. Este principio de la mecánica cuántica impide copiar de manera fiable la información cuántica a menos que se conozca la base en la que está codificada, cualquier dispositivo de copia de la información cuántica dependen de la base. Copiar con un dispositivo incorrecto no solo no produce una copia precisa, sino que también cambia el original de la misma manera que lo hace la medición con una base incorrecta y de nuevo Bob y Alice detectarían el ataque.

La seguridad de este protocolo, al igual que otros protocolos de distribución de claves clásicos, si es vulnerable a un ataque en el que Eve se hace pasar por Bob frente a Alice y se hace pasar por Alice frente a Bob. Para protegerse contra un ataque de este tipo, Alice y Bob deben combinar el protocolo con otro de autenticación.

3.3 Espacio de estados de un bit cuántico

El espacio de estados de un sistema físico clásico o cuántico es el conjunto de todos los estados posibles del sistema. Dependiendo de las propiedades del sistema que se consideren, un estado del sistema consiste en cualquier combinación de las posiciones, momentos, polarizaciones, espines, energía, etc. de las partículas del sistema. Si tenemos en cuenta unicamente la propiedad de polarización de un fotón, el espacio de estados estará formado por todas las polarizaciones posibles. De manera más general, el espacio de estados de un bit cuántico, con independencia de su implementación, es el conjunto de los posibles valores del cúbit, $a|0\rangle + b|1\rangle$, donde: $|a|^2 + |b|^2 = 1$ y $a|0\rangle + b|1\rangle$ y $a'|0\rangle + b'|1\rangle$ se consideran el mismo estado si $a|0\rangle + b|1\rangle = c(a'|0\rangle + b'|1\rangle)$

para cualquier numero complejo c de modulo 1.

Así, por ejemplo, el estado:

$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ y el estado: $\frac{i}{\sqrt{2}}(|0\rangle - |1\rangle)$ se consideran el mismo estado y:

$|\frac{i}{\sqrt{2}}|^2 + |\frac{-i}{\sqrt{2}}|^2 = |\frac{\sqrt{-1}}{\sqrt{2}}|^2 + |\frac{-\sqrt{-1}}{\sqrt{2}}|^2 = |\frac{-1}{2}| + |\frac{1}{2}| = 1$

3.4 Fase relativa y fase global

Un mismo estado cuántico puede ser representado por más de un vector en el espacio de estados y por tanto existe una diferencia fundamental entre el espacio vectorial complejo que utilizamos para describir el valor del cúbit y el espacio de estados cuánticos en sí. Hemos reducido la ambigüedad al exigir que los vectores que representan los estados cuánticos sean vectores unitarios, pero queda cierta ambigüedad: dos vectores unitarios equivalentes (múltiplos de un número complejo de modulo 1) representan el mismo estado. El múltiplo por el cual dos vectores que representan el mismo estado cuántico se diferencian se llama fase global y no tiene significado físico. La siguiente figura muestra esta equivalencia visualmente:

Figura 2: Dos versiones, con distinta fase global, del mismo estado. Elaboración propia.

Usamos la relación de equivalencia $|v\rangle \sim |v'\rangle$ para indicar que $|v\rangle = c|v'\rangle$ para alguna fase global compleja $c = e^{i\varphi}$. El espacio en el que dos vectores complejos bidimensionales se consideran equivalentes si son múltiplos entre sí se denomina espacio

proyectivo complejo de dimensión uno.

Debido a que la linealidad de los espacios vectoriales hace que sea más fácil trabajar con ellos que con los espacios proyectivos (sabemos cómo sumar vectores y no hay una forma correspondiente de sumar puntos en los espacios proyectivos), realizamos los cálculos en el espacio vectorial correspondiente al espacio de estados. Esta multiplicidad en la representación del estado puede ser una fuente de confusión. La fase global no tiene significado físico pero la fase relativa si la tiene. La fase relativa de una superposición $a|0\rangle + b|1\rangle$ es una medida del ángulo en el plano complejo entre los dos números complejos a y b. De forma más precisa, la fase relativa es el número complejo de módulo 1, $e^{i\varphi}$, que satisface: $\frac{a}{b} = e^{i\varphi}\frac{|a|}{|b|}$. Dos superposiciones $a|0\rangle + b|1\rangle$ y $a'|0\rangle + b'|1\rangle$ cuyas amplitudes tienen la misma magnitud pero que difieren en una fase relativa representan estados diferentes. La fase relativa, físicamente significativa y la fase global, sin significado físico, no deberían confundirse. Si bien la multiplicación por una constante unitaria no cambia un vector de estado cuántico, distintas fases relativas representan estados cuánticos distintos: aunque $|v1\rangle \sim e^{i\varphi}|v1\rangle$, los vectores $\frac{1}{\sqrt{2}}(e^{i\varphi}|v1\rangle + |v2\rangle)$ y $\frac{1}{\sqrt{2}}(|v1\rangle + |v2\rangle)$ no representan el mismo estado y deberemos ser conscientes de la equivalencia $\sim$ cuando interpretamos los resultados de nuestros cálculos como estados cuánticos.

Algunos estados los utilizaremos con tanta frecuencia que que resulta conveniente asignarles etiquetas especiales:

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

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

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

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

La base $|+\rangle, |-\rangle$ se conoce como la base Hadamard. Cuando trabajamos con fotones solemos utilizar la notación $|\nwarrow\rangle, |\nearrow\rangle$ para referirnos a la base de Hadamard. Escribiremos siempre explícitamente los factores de normalización, esto ayuda a verificar los cálculos y evitar errores y proporciona una relación directa entre las amplitudes y las probabilidades en la medición.

3.5 Visualización del espacio de estados del cúbit

Si bien utilizamos principalmente vectores para representar estados cuánticos, es útil tener modelos del espacio de estados de un solo qubit en el que hay una correspondencia uno a uno entre estados y puntos en el espacio. Estos modelos son simplemente diferentes formas de ver el espacio proyectivo complejo de dimensión 1. Como veremos, el espacio proyectivo complejo de dimensión 1 puede verse como una esfera. Primero mostramos que se puede ver como el plano complejo extendido, el plano complejo C junto con un punto adicional tradicionalmente etiquetado como ∞.

Plano complejo extendido $C \bigcup \infty$

Una correspondencia entre el conjunto de los números complejos y los estados de un cúbit viene dada por:

$$a|0\rangle + b|1\rangle \Rightarrow \frac{b}{a} = \alpha$$

Y su inversa:

$$\alpha \Rightarrow \frac{1}{\sqrt{1+|\alpha|^2}}|0\rangle + \frac{\alpha}{\sqrt{1+|\alpha|^2}}|1\rangle$$

La correspondencia anterior no está definido para el estado con $a = 0$ y $b = 1$. Para hacer esta correspondencia uno a uno, necesitamos agregar un punto al plano complejo que denominaremos ∞ y definir $\infty \iff |1\rangle$. Por ejemplo, tenemos:

$$|0\rangle \Longmapsto 0$$

$$|1\rangle \Longmapsto \infty$$

$$|+\rangle \Longmapsto +1$$

$$|-\rangle \Longmapsto -1$$

$$|i\rangle \Longmapsto i$$

$$|-i\rangle \Longmapsto -i$$

A continuación describimos otro modelo relacionado con el anterior, la esfera de Bloch.

La esfera de Bloch

A partir de la representación anterior, podemos hacer corresponder cada estado, representado por el número complejo $\alpha = s + it$, sobre la esfera unitaria en tres dimensiones reales, los puntos $(x, y, z) \in C$que satisfacen $|x|^2 + |y|^2 + |z|^2 = 1$, utilizando la proyección estereográfica estándar:

$(s, t) \Rightarrow (\frac{2s}{1+|\alpha|^2}, \frac{2t}{1+|\alpha|^2}, \frac{1-|\alpha|^2}{1+|\alpha|^2})$

exigiendo de nuevo que: $\infty \Longmapsto (0, 0, -1)$

La siguiente figura muestra la esfera de Bloch y sus correspondencias:

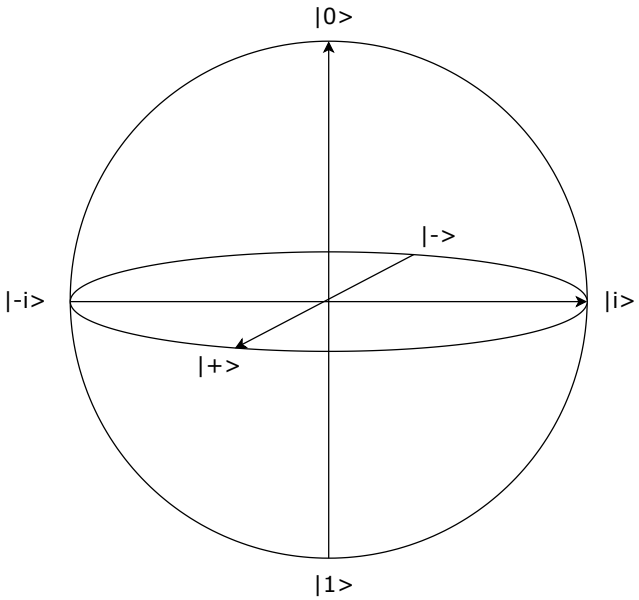


Figura 3: Esfera de Bloch. Elaboración propia.

$|0\rangle \Longmapsto (0, 0, 1)$

$|1\rangle \Longmapsto (0, 0, -1)$

$|+\rangle \Longmapsto (1, 0, 0)$

$|-\rangle \Longmapsto (-1, 0, 0)$

$|i\rangle \Longmapsto (0, 1, 0)$

$|-i\rangle \Longmapsto (0,-1,0)$

Hemos dado tres representaciones del espacio de estados de un cubit. Como vectores escritos en la notación Bra-Ket: $a|0\rangle + b|1\rangle$ con coeficientes complejos a y b, con la restricción de normalización $|a|^2 + |b|^2 = 1$, donde a y b son únicos excepto por un factor unitario complejo . Debido a este factor, que corresponde con la fase global, esta representación no es uno a uno; sobre el plano complejo extendido con un solo número complejo $\alpha \in C$ o $\alpha \in \infty$, esta representación es uno a uno y por último con la esfera de Bloch co o puntos (x, y, z) en la esfera unitaria, esta representación también es uno a uno. Por razones históricas, la esfera, incluyendo su interior, cuyos puntos tienen también significado, se denomina esfera de Bloch, en lugar de solo los puntos de la superficie. Por esta razón, nos referimos al espacio de estados de un qubit como la superficie de la esfera de Bloch.

Utilizando el entorno de desarrollo de QISKit, realiza el siguiente experimento que muestra la visualización del estado utilizando la Esfera de Bloch.

Ejemplo 1. Visualización del estado usando la Esfera de Bloch

```
#Importar librerías

from qiskit import QuantumRegister, QuantumCircuit

from qiskit.visualization import plot_bloch_multivector

# Construcción del registro cuántico de 1 qubit y del circuito

qr = QuantumRegister(1)

my_circuit = QuantumCircuit(qr)

# Aplicamos una puerta de Hadamard al qubit

my_circuit.h(0)

# Visualizamos el circuito
```

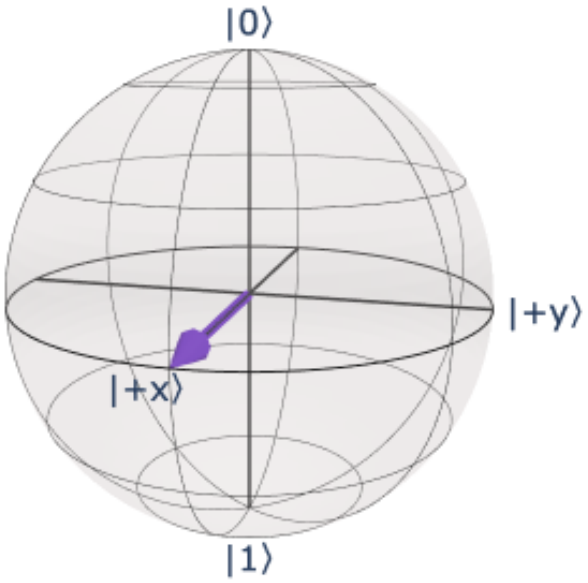
```
my_circuit.draw())
```

```
q[0]  |0>  ┤ H ├
```

```
# Inicialización a |0>y evolución a través del circuito

from qiskit.quantum_info import Statevector

state = Statevector.from_int(0, 2)

state = state.evolve(my_circuit)

state.draw('latex')
```

$$\left[\frac{1}{\sqrt{2}} \quad \frac{1}{\sqrt{2}}\right]$$

```
plot_bloch_multivector(state,title="Blochsphere")
```



Una de las ventajas de la representación de la esfera de Bloch es que es fácil identifi-

car todas las bases posibles del modelo ya que los estados ortogonales corresponden a puntos opuestos de la esfera de Bloch, así cada diámetro de la esfera de Bloch corresponde a una base para el espacio de estados del qubit. La siguiente figura difiere de la representación de la esfera de Bloch en que los ángulos son la mitad que los de la representación de la esfera de Bloch, el ángulo entre dos estados tiene su relación habitual con el producto interno, mientras que en la representación de la esfera de Bloch el ángulo es el doble.

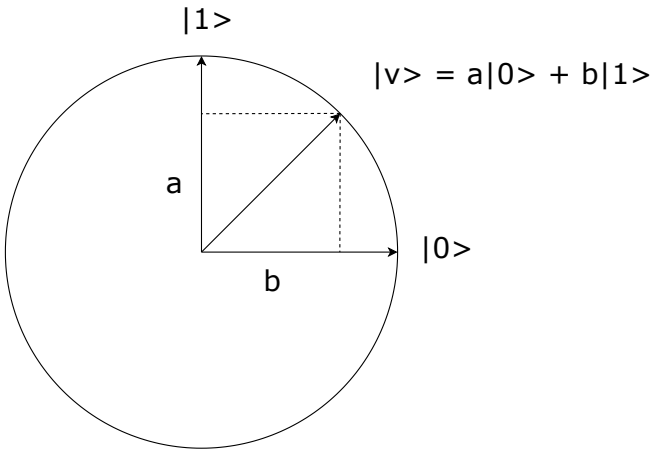


Figura 4: Representación del estado sin considerar la parte imaginaria de los coeficientes.

Un bit clásico tiene únicamente un parámetro binario, podemos establecer el bit en uno de los dos posibles estados, lo cual hace que la lógica binaria sea muy simple.

Representación con círculos

Podríamos también representar visualmente los valores 0 y 1 de un bit mediante círculos separados, vacíos o llenos, como se muestra en la siguiente figura, donde se muestran los posibles valores del bit clásico.

Figura 5: Bit clásico. Elaboración propia.

En cierto sentido los bits cuánticos son semejantes a los bits clásicos, al leer el valor

del cíbit se obtiene siempre 0 o 1, por tanto, tras la lectura, podremos describir el cúbit como en la figura anterior. Sin embargo, la caracterización del bit cuántico *antes* de la lectura requiere una descripción más sofisticada ya que el cúbit puede existir en una superposición de estados, la siguiete figura muestra algunos estados posibles de un cúbit utilizando la notación de círculos.

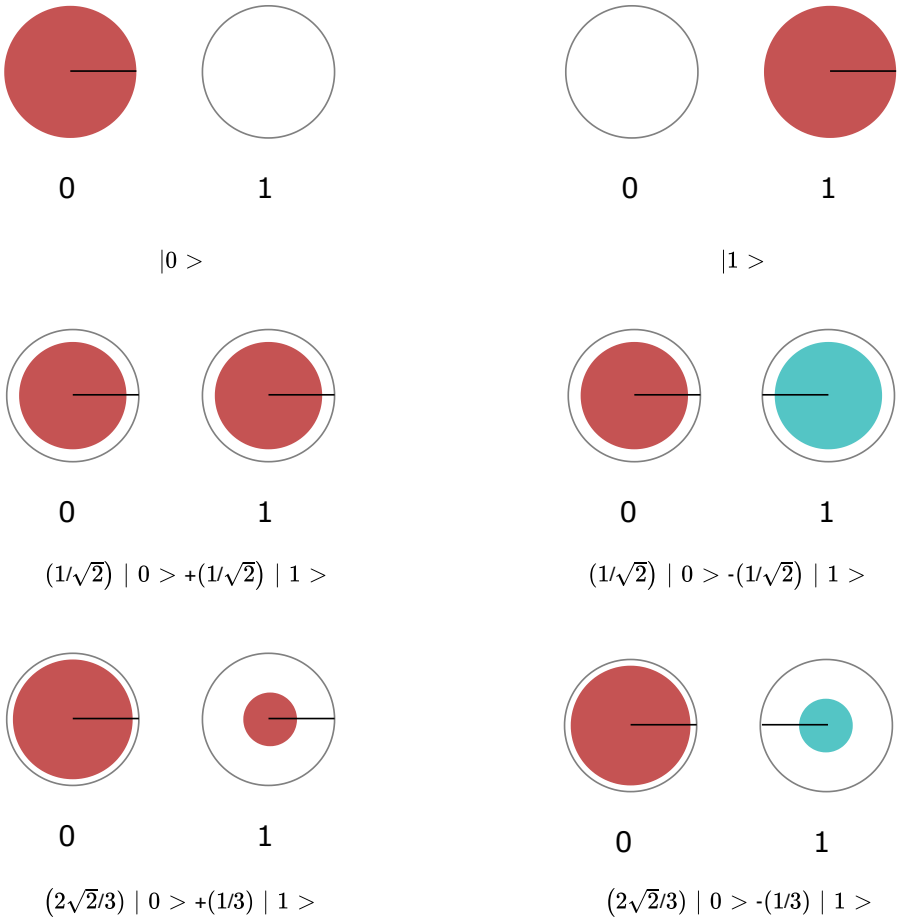


Figura 6: Ejemplos de estados cuánticos del cúbit. Elaboración propia.

Las dos primeras filas muestran las versiones cuánticas de los estados de un bit clásico, sin superposición. Las tres restantes son tres posibles estados en superposición del cúbit. Esta representación intuitiva del estado del cúbit nos permitirá visualizar no solo el estado de un cúbit sino de un conjunto de ellos. De todo lo estudiado hasta el momento sabemos que hay dos aspectos del estado general del cúbit que nos interesan: la magnitud de las amplitudes y la fase relativa entre ellas, la visualización del estado basado en circulos las representa de la siguiente forma:

La magnitud de la amplitud asociada a los dos vectores de la base $|0\rangle, |1\rangle$ está relacionada con el radio de la parte rellena de color de los círculos correspondientes a $|0\rangle$ y $|1\rangle$. La fase relativa entre las amplitudes, la rotación del circulo correspondiente al $|1\rangle$ relativa al circulo correspondiente al $|0\rangle$, se representa de dos formas, por un lado con un radio negro y por otro con el color, que sigue el siguiente patrón:

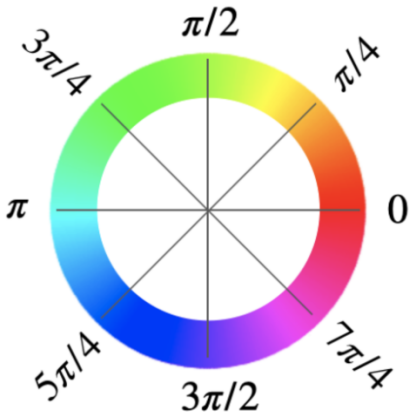


Figura 7: Rueda de color. Elaboración propia.

Como hemos visto, el cuadrado de la magnitud asociada a $|0\rangle$ o $|1\rangle$ determina la probabilidad de obtener ese valor en la lectura. Ya que el radio del circulo relleno representa la magnitud, quiere decir que el área rellena del circulo es directamente proporcional a la probabilidad de obtener ese resultado en la lectura. La siguiente figura muestra algunos ejemplos en la notación de círculos para diferentes estados y la probabilidad de leer 1 en cada caso.

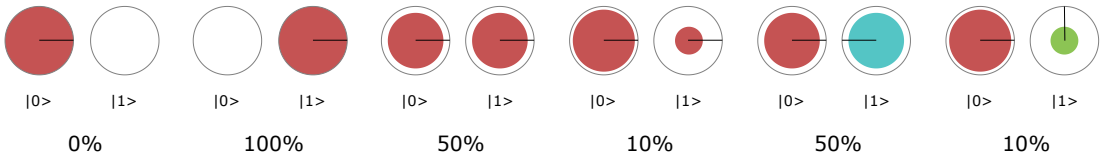


Figura 8: Probabilidad de leer 1 para diferentes estado. Elaboración propia.

A medida que el área sombreada asociada al $|0\rangle$aumenta, la probabilidad de obtener 0 en la medida se hace mayor y por tanto la probabilidad de obtener 1 disminuye. Es importante recordar que le tamaño del circulo no representa de forma completa la amplitud, la información que falta es la correspondiente a la fase relativa. La fase relativa del estado de un cúbit puede tomar cualquier valor de 0˚ a 360˚, la siguiente

figura muestra algunos ejemplos.

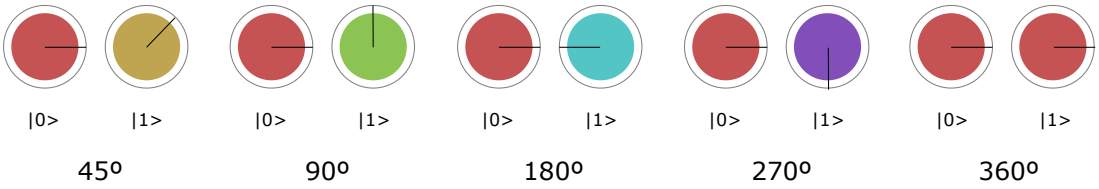


Figura 9: Ejemplos de fase relativa. Elaboración propia.

En estos ejemplos se ha rotado únicamente el circulo correspondiente al $|1\rangle$, ya que se trata de la fase *relativa* de la superposición y por tanto solo la rotación relativa entre los círculos tiene significado, como se puede ver en la siguiente figura.

Figura 10: Equivalencia entre estados con diferente fase global. Elaboración propia.

Hay que tener en cuenta que la fase relativa se puede variar de forma independiente a la magnitud de una superposición. Esta independencia también funciona al revés, en los ejemplos, podemos ver que la fase relativa no tiene un efecto directo sobre las probabilidades de los resultados del proceso de medida. Este hecho de que la fase relativa de un cubit no tenga efecto sobre la magnitud de una superposición significa que no tiene una influencia directa en los resultados y puede hacer que la propiedad de fase relativa parezca irrelevante, sin embargo, no podría ser más diferente. En la computación cuántica que involucra múltiples cubits, podemos aprovechar esta rotación como una herramienta fundamental para alterar de manera inteligente e indirecta las probabilidades los resultados de la medida, de hecho, el uso de las fases relativas pueden proporcionar una ventaja computacional asombrosa.

Los estados de todos los sistemas cuánticos satisfacen ciertas propiedades que están modeladas por una ecuación diferencial lineal llamada ecuación de onda de Schrödinger. Las soluciones a la ecuación de Schrödinger se denominan funciones de onda, por

lo que todos los estados cuánticos tienen representaciones como funciones de onda. Podemos ver las funciones de onda como vectores abstractos que representaremos con kets, tal y como $|\Psi\rangle$.

Dado que la ecuación de Schrödinger es lineal, la suma de dos soluciones de la ecuación de Schrödinger o un múltiplo constante de una solución de la ecuación de Schrödinger, son también soluciones. El conjunto de soluciones de la ecuación de Schrödinger, para cualquier sistema cuántico, es un espacio vectorial complejo y además, el conjunto de soluciones, tiene un producto interior.

En computación cuántica, en general, es suficiente considerar sólo espacios vectoriales de dimensión finita, si la dimensión es infinita, el espacio de soluciones satisface las condiciones necesarias para formar un espacio de Hilbert. A menudo se mencionan los espacios de Hilbert al hablar de computación cuántica, ya que son el caso más general, pero en general, los espacios de Hilbert discutidos no son de dimensión infinita y por tanto no son sino espacios vectoriales complejos de dimensión finita.

3.6 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