
Curso de Formación Continua en Computación Cuántica
Organizado por la Escuela Politécnica de Cáceres.
Universidad de Extremadura

# Curso de Computación cuántica 6.0

## Fundamentos y puertas de uno y dos qubits

Fernando Cuartero

Escuela Superior de Ingeniería Informática
Universidad de Castilla-La Mancha

# Indice

## Computación Cuántica. Un nuevo paradigma

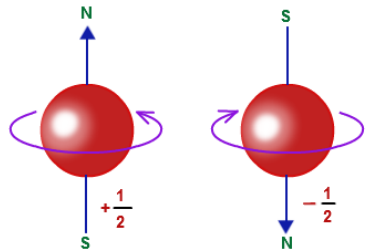
- ✔ Se basa en el uso de qubits en lugar de bits
- ✔ Nuevas puertas lógicas que hacen posibles nuevos algoritmos y métodos de cómputo
- ✔ Se pueden resolver problemas hasta ahora sin solución
- ✔ Puede llegar allá donde la Ley de Moore ya no permite avanzar más

## Computación Cuántica. Un nuevo paradigma

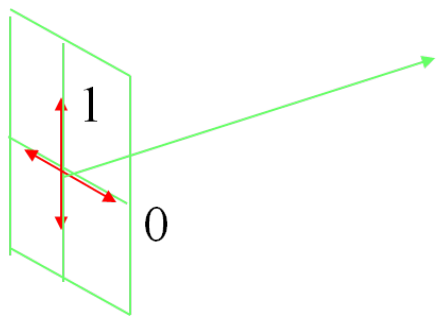
- ✔ **Información Clásica**
  - ✗ Se reduce a 1´s y 0´s
  - ✗ Se guardan en memorias magnéticas, ópticas ...
  - ✗ Se transmiten por pulsos eléctricos, luz...
- ✔ **Información Cuántica**
  - ✗ No se reduce a 1´s y 0´s
  - ✗ Se guarda y se transmite por estados cuánticos
  - ✗ Entrelazamiento
  - ✗ Aplicaciones: Encriptación, Paralelismo...
  - ✗ Uso de algoritmos aleatorios

## Computación Cuántica. Un nuevo paradigma

- ✔ ¿Cual es el espacio mínimo para almacenar información?
- ✔ Podemos usar el spin de un electrón




- ✔ Podemos usar la polarización de un fotón




Pero esto tiene efectos colaterales

## Preliminares

- ✔ **Historia**
  - ✗ 1927 Principio de indeterminación de Heisenberg
  - ✗ 1935 Artículo Einstein-Podolsky-Rosen
  - ✗ 1964 Teorema de Bell
  - ✗ 1970 Teoría de las medidas cuánticas
  - ✗ 1961 Experimento de Alain Aspect en París
  - ✗ 1982 Richard Feynman: Simulating physics with computers
  - ✗ 1985 David Deutsch: Modelo de circuitos
  - ✗ 1998 Cirac y Zoller desarrollan el primer qbit, basado en trampa de iones
  - ✗ 2002 Se implementa la primera puerta CNot

## Preliminares

- ✔ **Historia**
  - ✗ El primero en considerar que la mecánica cuántica podía ser aplicable a resolver sistemas de cómputo es Richard Feynman
  - ✗ Observa que el coste computacional de simular sistemas cuánticos crece de manera exponencial con el tamaño del sistema
  - ✗ Si consideramos que un sistema está calculando su propia evolución, y puesto que lo hace en un tiempo mucho menor, entonces está resolviendo un problema exponencial en un tiempo limitado
  - ✗ En 1985, David Deutsch introduce el modelo de circuitos de computación cuántica actualmente adoptado como estándar
  - ✗ Deutsch también muestra que todo operador cuántico puede ser definido composicionalmente a partir de un reducido número de operadores universales

## Preliminares

- ✔ **Argumento fundamental**
  - ✗ Richard Feynman en *Simulating Physics with Computers*, International Journal of Theoretical Physics, 1982.
  - ✗ La simulación de la estructura cuántica del átomo, calculando la distribución de energías de los diferentes orbitales, necesita un tiempo exponencial en el número de niveles y partículas.
  - ✗ Sin embargo, un átomo lo hace directamente.
  - ✗ Eso significa que el átomo, actuando como computador, puede resolver un problema de naturaleza exponencial en un corto espacio de tiempo.
  - ✗ La cuestión es... ¿Puede esto generalizarse?

**4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS**

The first branch, one you might call a side-remark, is, Can you do it with a new kind of computer—a quantum computer? (I'll come back to the other branch in a moment.) Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind. If we disregard the continuity of space and make it discrete, and so on, as an approximation (the same way as we allowed ourselves in the classical case), it does seem to

## Preliminares

### ✔ Idea de Feynman

- ✗ Con el modelo atómico de Bohr, y por medio de la ecuación de Schrödinger se puede calcular el nivel de energía de un átomo de Hidrógeno. Tiene un electrón, y se necesita resolver un hamiltoniano de una matriz de $2 \times 2$
- ✗ La molécula de agua es algo más difícil. El $H_2O$ tiene 10 electrones, y el hamiltoniano es una matriz de $2^{10} \times 2^{10}$, más de un millón de componentes numéricas. Se puede resolver, pero toma un tiempo importante.
- ✗ La molécula de alcohol, $CH_3CH_2OH$ tiene 26 electrones, por lo que el hamiltoniano es una matriz de $2^{26} \times 2^{26}$. El cálculo del nivel de energía. Esto son mil billones de componentes numéricas, y ya supone un esfuerzo muy importante de supercomputación, que puede tomar horas.
- ✗ Richard Feynman se plantea, una molécula de alcohol, que es algo muy pequeño, cuando arde, realiza ese cálculo en una fracción de segundo.
- ✗ Una molécula realiza cálculos enormes en un tiempo minúsculo... ¿Podemos aprovecharlo?

## Teoría Cuántica

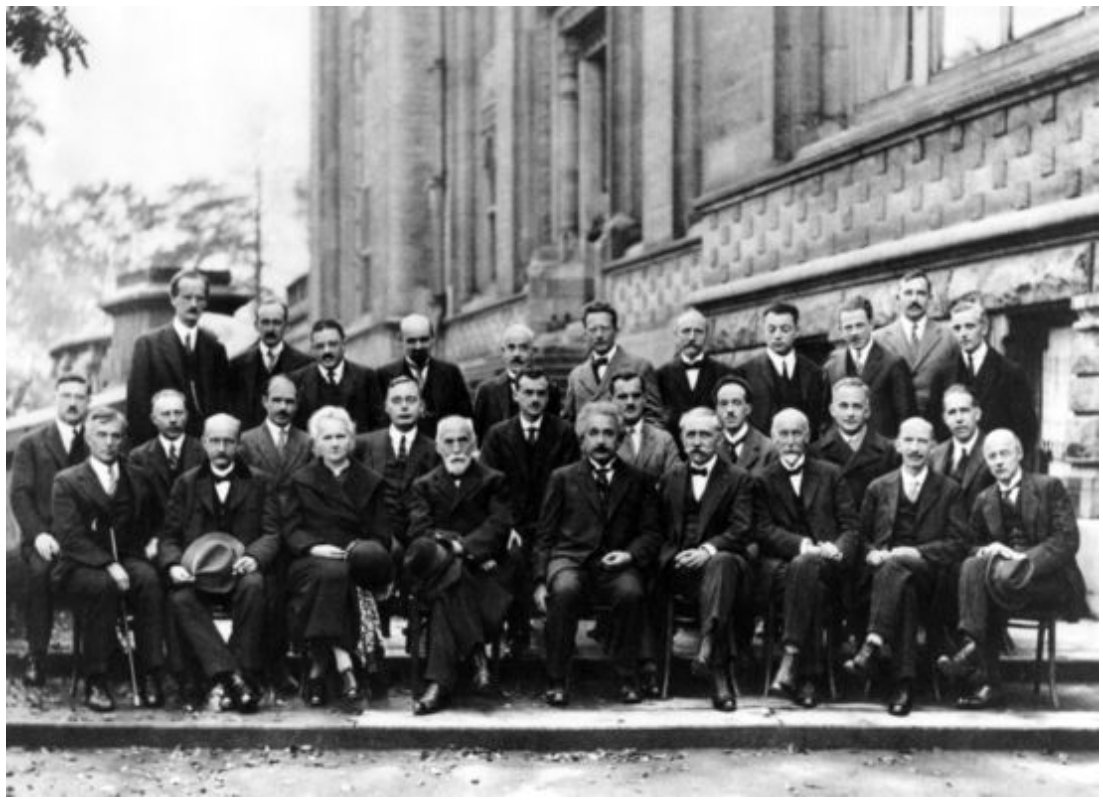
- *Cualquiera que no esté impactado con la teoría cuántica es que no la ha entendido.*
  Niels Bohr
- *Pienso que se puede afirmar tranquilamente que nadie entiende la mecánica cuántica.*
  Richard Feynman

## ¿Qué es la Mecánica Cuántica?

- ✔ La Mecánica Cuántica es una teoría. Es el modelo estandar que describe el comportamiento de la materia y la energía a escalas pequeñas (fotones, átomos, núcleos, quarks, gluones, leptones ...)
- ✔ Una teoría consiste en un **formalismo** matemático, junto a una **interpretación** del mismo
- ✔ Sin embargo, al contrario que otras teorías, la Mecánica Cuántica difiere en que, mientras que su formalismo ha sido aceptado y usado durante 80 años, su interpretación permanece en continua controversia y debate

# ¿Qué es la Mecánica Cuántica?

- ✔ Interpretaciones
- ✔ El primer debate tuvo lugar durante la quinta Conferencia Solvay de 1927, en Bruselas



## ¿Qué es la Mecánica Cuántica?

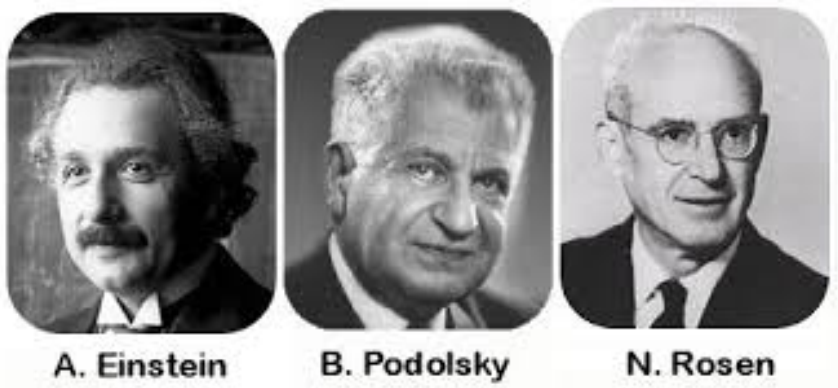
- ✔ Interpretaciones
- ✔ ¿Cual es correcta?

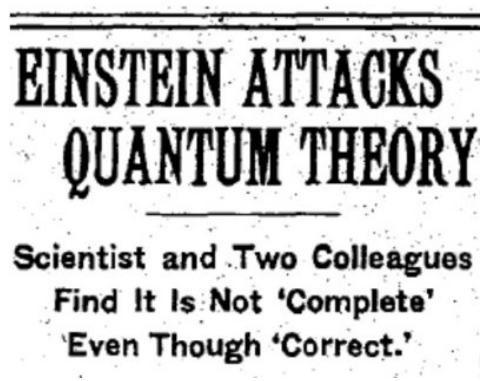
Debates Bohr-Einstein

La mecánica cuántica: un modelo de ciencia no-determinista o una teoría probabilística incompleta

## Paradoja. Experimento EPR

- ✔ Albert Einstein tenía un problema personal con la física cuántica. A pesar de haber contribuido a su gestación, no la aceptaba.
- ✔ En 1935, junto a dos estudiantes de doctorado suyos publica un experimento mental con el objetivo de refutar sus postulados.
- ✔ Sin embargo, los resultados no fueron los esperados...


A. Einstein B. Podolsky N. Rosen

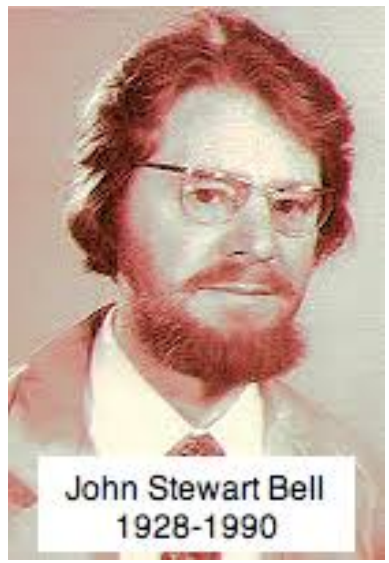

EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

## Paradoja. Experimento EPR

- ✔ El debate Einstein-Bohr fue zanjado mediante el experimento EPR
- ✔ En 1964 John S. Bell presenta el teorema de las desigualdades, o teorema de Bell que dice:

  *"Ninguna teoría física de variables ocultas locales puede reproducir todas las predicciones de la mecánica cuántica"*
- ✔ Puede ser comprobado experimentalmente. Fue llevado a cabo por Alain Aspect en 1981



## Números complejos

- Los números complejos, designados con $\mathbb{C}$, son una extensión de los números reales. Un número complejo está formado por dos números reales, respectivamente denominados parte real y parte imaginaria
- Se construyen a partir de la unidad imginaria, denominada con la letra $i$, que cumple la propiedad de que $i^2 = -1$
- Otra propiedad, que se sigue de la anterior, es que los números complejos incluyen todas las raíces de los polinomios con coeficientes reales
- Representación en forma polinómica: Habitualmente un número complejo se representa mediante la composición de la parte real y la imaginaria en la forma

$$c \in \mathbb{C} \rightarrow c = a + b \cdot i \ a, b \in \mathbb{R}$$

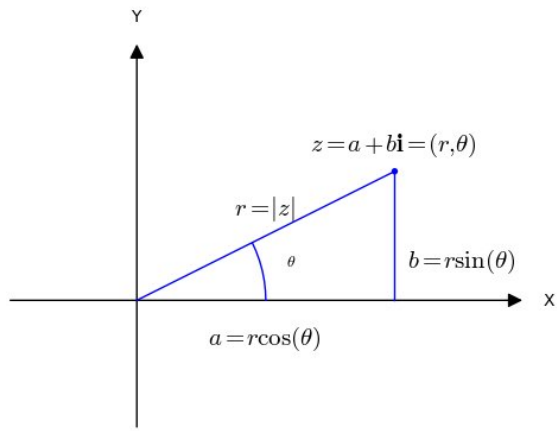
## Números complejos

- ✔ Forma Polar. Dado un número complejo $z = a + b \cdot i$, podemos definir dos valores asociados, el módulo y el argumento, en la forma
- ✔ Módulo

$$|z| = \sqrt{a^2 + b^2}$$

- ✔ Argumento

$$\cos\theta = a/|z|$$




$$z = |z| \cdot (\cos\theta + i \cdot \sin\theta)$$

## Números complejos

- ✔ Fórmula de Moivre. Si tenemos un número complejo de módulo 1 se satisface:

$$(\cos\theta + \sin\theta \cdot i)^n = \cos(n \cdot \theta) + \sin(n \cdot \theta) \cdot i$$

- ✔ Forma exponencial

$$z = |z| \cdot e^{\theta \cdot i}$$

- ✔ Fórmula de Euler

$$e^{\pi \cdot i} + 1 = 0$$

## Números complejos

- ✔ La forma exponencial nos permite realizar muchas más operaciones sobre los números complejos, entre ellas el logaritmo o la exponencial
- ✔ Curiosidad

$$\begin{aligned} \log -1 &= ? \\ i^i &= ? \end{aligned}$$

## Números complejos

- ✔ La forma exponencial nos permite realizar muchas más operaciones sobre los números complejos, entre ellas el logaritmo o la exponencial
- ✔ Curiosidad

$$\begin{aligned} \log -1 &= \log\left(e^{\pi \cdot i}\right) \\ &= \pi \cdot i \end{aligned}$$

$$\begin{aligned} \log i &= \log\left(e^{\pi/2 \cdot i}\right) \\ &= \pi/2 \cdot i \end{aligned}$$

## Números complejos

- ✔ La forma exponencial nos permite realizar muchas más operaciones sobre los números complejos, entre ellas el logaritmo o la exponencial
- ✔ Curiosidad

$$\begin{aligned} i^i &= (e^{\frac{\pi}{2} i})^i \\ &= e^{\frac{\pi}{2} i \cdot i} \\ &= e^{\frac{\pi}{2} i^2} \\ &= e^{-\frac{\pi}{2}} \end{aligned}$$

- ✔ Es decir, el valor $i^i$ es un número real puro, sin componente imaginaria, y su valor aproximado es 0.02079

## Álgebra lineal

Un **espacio vectorial** sobre el espacio de los números complejos está formado por vectores, que son tuplas de la forma $(z_1, \ldots, z_n)$. En computación cuántica, usaremos la notación $|Q\rangle$ para representar el vector columna $Q$

$$|Q\rangle = \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}$$

## Álgebra lineal

En un espacio vectorial podemos definir operaciones de adición y producto por un número

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z'_1 \\ \vdots \\ z'_n \end{bmatrix} = \begin{bmatrix} z_1 + z'1 \\ \vdots \\ z_n + z'_n \end{bmatrix}$$

$$z \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} = \begin{bmatrix} z\, z_1 \\ \vdots \\ z\, z_n \end{bmatrix}$$

## Álgebra lineal

Tabla resumen de notación

| Notación | Contenidos |
|---|---|
| $z^*$ | Complejo conjugado del número $z$. Parte imaginaria cambiada de signo. Ej. $(1+i)^* = 1-i$ |
| $\|Q\rangle$ | Vector columna (*Ket*) |
| $\langle Q\|$ | Vector dual (fila o *Bra*) |
| $\langle Q_1\|Q_2\rangle$ | Producto interno (escalar) |
| $\|Q_1\rangle\langle Q_2\|$ | Matriz de densidad |
| $\|Q_1\rangle \otimes \|Q_2\rangle$ | Producto tensorial |
| $\|Q_1\rangle\|Q_2\rangle$ | Producto tensorial. Forma abreviada |
| $A^*$ | Matriz conjugada de $A$ |
| $A^T$ | Matriz traspuesta de $A$ |
| $A^\dagger$ | Matriz traspuesta conjugada de $A$, es decir $A^\dagger = (A^T)^*$ |

## Álgebra lineal

Ejemplo. El producto tensorial de dos vectores de dimensión 2 es un vector de dimensión 4

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \otimes \begin{bmatrix} z'_1 \\ z'_2 \end{bmatrix} = \begin{bmatrix} z_1 \cdot z'1 \\ z_1 \cdot z'2 \\ z_2 \cdot z'1 \\ z_2 \cdot z'2 \end{bmatrix}$$

## Álgebra lineal

- ✔ Un conjunto de vectores no nulos $(\{|v_1\rangle, \ldots, |v_n\rangle\}$ son linealmente dependientes si existe un conjunto de números complejos $a_1, \ldots, a_n$ con $a_i \neq 0$ para al menos algún $i$, tales que

$$a_1|v_1\rangle + a_2|v_2\rangle + \ldots + a_n|v_n\rangle = 0$$

- ✔ Un conjunto de vectores es linealmente independiente si no es linealmente dependiente
- ✔ Una base de un espacio vectorial es un conjunto de vectores linealmente independiente, y tal que cualquier vector puede expresarse como combinación lineal de ellos
- ✔ Un operador lineal entre dos espacios vectoriales $V$ y $W$ es una función $A$ que es lineal respecto a sus entradas

$$A\sum_i |v_i\rangle = \sum_i A|v_i\rangle$$

## Álgebra lineal

- Las matrices de Pauli son unas matrices de dimensión 2, operadores lineales, muy usadas en mecánica cuántica

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Un autovector de un operador lineal $A$ es un vector no nulo $|v\rangle$ tal que existe un número complejo $z$ tal que

$$A|v\rangle = z|v\rangle$$

$z$ es conocido como autovalor

## Álgebra lineal

- ✔ Un espacio de Hilbert es un espacio vectorial dotado de una función de medida (módulo) y una noción de ortogonalidad.
- ✔ Ambas nociones se introducen mediante un producto escalar sobre un cuerpo. En este caso los números complejos
- ✔ Los elementos del espacio de Hilbert se suelen representar usando la notación de Dirac en forma de columna (*ket*)

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

- ✔ o de fila (*bra*), en este caso, los conjugados.

$$\langle 0| = [1\ 0], \quad \langle 1| = [0\ 1]$$

$$\langle \psi| = [a^\dagger\ \ b^\dagger]$$

## Álgebra lineal

- ✔ El producto $\langle\psi| \cdot |\psi\rangle = \langle\psi|\psi\rangle$ es un número complejo
- ✔ Operaciones en el espacio de Hilbert
  - ✗ Producto de matrices
  - ✗ Producto vectorial
  - ✗ Producto escalar
  - ✗ Matriz de densidad $|\psi\rangle\langle\psi|$

$$|0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

## Álgebra lineal

- ✔ Producto de Kronecker. Es un caso especial del producto tensorial de matrices
- ✔ Como el producto tensorial, se denota por $\otimes$, y se aplica a dos matrices $A$, $B$ de tamaño arbitrario, respectivamente $m \times n$ y $p \times q$
- ✔ El resultado es una matriz $A \otimes B$ de tamaño $(m \cdot p) \times (n \cdot q)$

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & \cdots & b_{1q} \\ \vdots & \ddots & \vdots \\ b_{p1} & \cdots & b_{pq} \end{bmatrix}$$

$$A \otimes B = \begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{11}b_{1q} & \cdots & \cdots & a_{1n}b_{11} & a_{1n}b_{12} & \cdots & a_{1n}b_{1q} \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{11}b_{2q} & \cdots & \cdots & a_{1n}b_{21} & a_{1n}b_{22} & \cdots & a_{1n}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \cdots & \vdots \\ a_{11}b_{p1} & a_{11}b_{p2} & \cdots & a_{11}b_{pq} & \cdots & \cdots & a_{1n}b_{p1} & a_{1n}b_{p2} & \cdots & a_{1n}b_{pq} \\ \vdots & \vdots & & \vdots & \ddots & & \vdots & \vdots & & \vdots \\ \vdots & \vdots & & \vdots & & \ddots & \vdots & \vdots & & \vdots \\ a_{m1}b_{11} & a_{m1}b_{12} & \cdots & a_{m1}b_{1q} & \cdots & \cdots & a_{mn}b_{11} & a_{mn}b_{12} & \cdots & a_{mn}b_{1q} \\ a_{m1}b_{21} & a_{m1}b_{22} & \cdots & a_{m1}b_{2q} & \cdots & \cdots & a_{mn}b_{21} & a_{mn}b_{22} & \cdots & a_{mn}b_{2q} \\ \vdots & \vdots & \ddots & \vdots & & & \vdots & \vdots & \ddots & \vdots \\ a_{m1}b_{p1} & a_{m1}b_{p2} & \cdots & a_{m1}b_{pq} & \cdots & \cdots & a_{mn}b_{p1} & a_{mn}b_{p2} & \cdots & a_{mn}b_{pq} \end{bmatrix}$$

# Álgebra lineal

Ejemplo, producto de Kronecker

$$\begin{bmatrix} 1 & 2 \\ 3 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 3 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1\cdot 0 & 1\cdot 3 & 2\cdot 0 & 2\cdot 3 \\ 1\cdot 2 & 1\cdot 1 & 2\cdot 2 & 2\cdot 1 \\ 3\cdot 0 & 3\cdot 3 & 1\cdot 0 & 1\cdot 3 \\ 3\cdot 2 & 3\cdot 1 & 1\cdot 2 & 1\cdot 1 \end{bmatrix} = \begin{bmatrix} 0 & 3 & 0 & 6 \\ 2 & 1 & 4 & 2 \\ 0 & 9 & 0 & 3 \\ 6 & 3 & 2 & 1 \end{bmatrix}$$

## Información cuántica

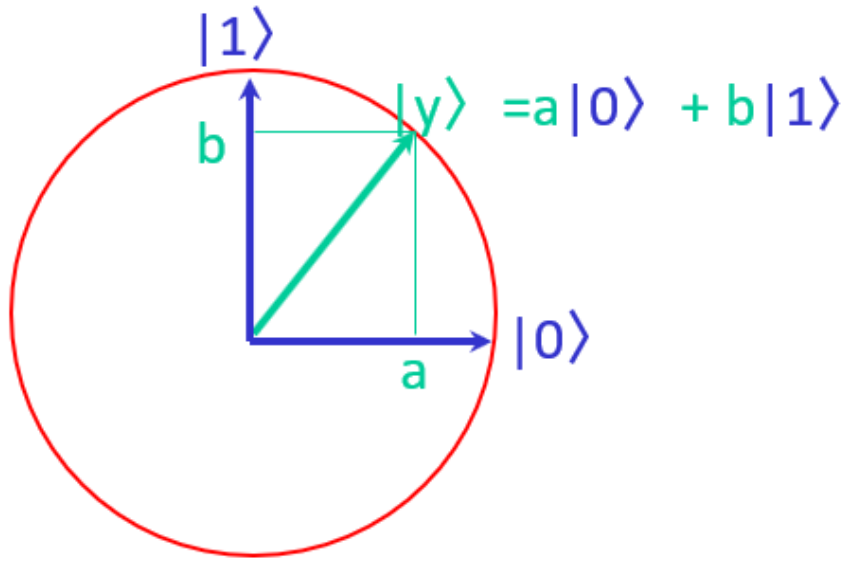
El estado de un qubit es un vector $|y\rangle = a|0\rangle + b|1\rangle$

- ✔ $a, b$ son números complejos tales que

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

- ✔ El vector $|y\rangle$ puede ser escrito como columnas (notación de Dirac)

$$|0\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |y\rangle = \begin{bmatrix} a \\ b \end{bmatrix}$$



## Información cuántica

- ✔ Matriz de densidad

$$|a\ b\rangle\langle a\ b| = \begin{bmatrix} a^2 & ab \\ ba & b^2 \end{bmatrix}$$

- ✔ Superposición

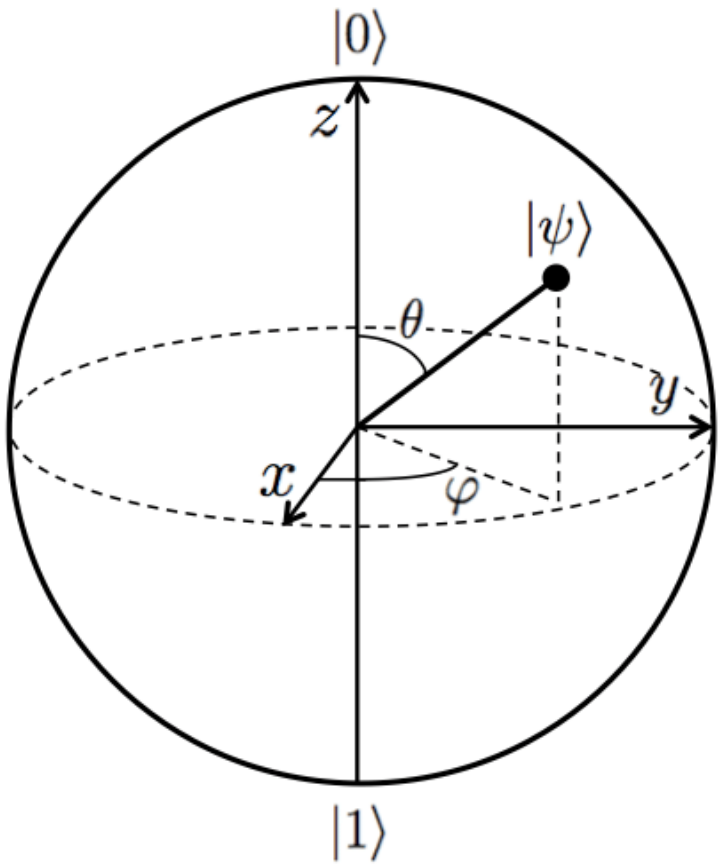
$$|a\ b\rangle = a|0\rangle + b|1\rangle$$

- ✔ $\{|0\rangle, |1\rangle\}$ forman una base del espacio de Hilbert
- ✔ En física cuántica, los vectores $|0\rangle$ y $|1\rangle$ se denominan **estados puros**. Las combinaciones lineales que forman el resto de elementos del espacio de Hilbert se denominan **estados mixtos**

## Esfera de Bloch

El estado de un qubit se puede representar mediante la esfera de Bloch

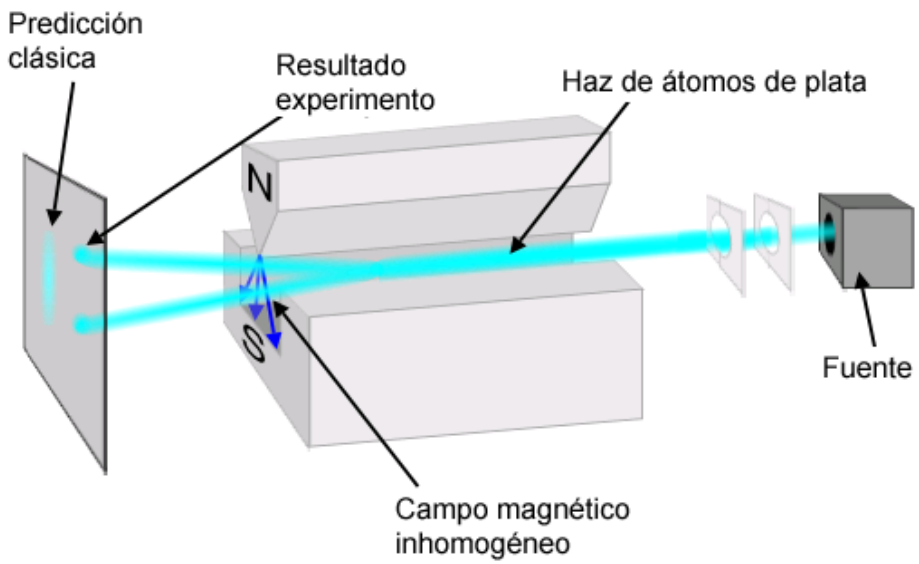
$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$



## Esfera de Bloch

### Experimento de Stern y Gerlach

- ✔ Reallizado en Francfort, en 1922 por Otto Stern y Walther Gerlach
- ✔ Consiste en enviar un haz de átomos en un medio dotado de un campo magnético, con el polo norte en la parte superior y polo sur en la inferior



## Esfera de Bloch

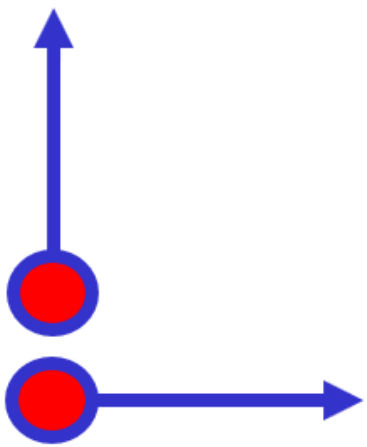
### Experimento de Stern y Gerlach

- **Predicción clasica**: Cada átomo tiene un momento magnético aleatorio, que le produce un desvío en su trayectoria, hacia arriba o hacia abajo. Se debe observar un impacto en una línea contínua vertical
- **Obervación real**: Sólo existen dos puntos de impacto, uno situado en una posición superior, y otro situado en otra inferior
- Por primera vez aparece el efecto del spin. El momento magnético solo puede tomar dos valores $+1/2$ y $-1/2$

# Información Cuántica

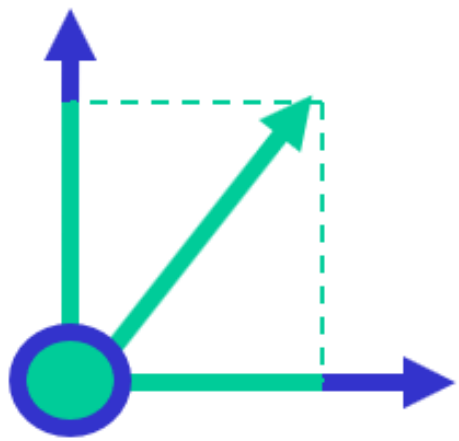
Un bit clásico en cada instante puede estar:

- ✔ En el estado 0
- ✔ En el estado 1
- ✔ $b \in \{0, 1\}$



Un bit cuántico en cada instante puede estar:

- ✔ En el estado base $|0\rangle$
- ✔ En el estado $|1\rangle$
- ✔ o en una superposición de estados de $|0\rangle$ y $|1\rangle$



## Esfera de Bloch

- En principio se necesitan cuatro coordenadas reales para representar un qubit, dos por cada valor complejo
- Sin embargo, dado un qubit de estado $|\psi\rangle = a|0\rangle + b|1\rangle$ su comportamiento es idéntico al de cualquier otro qubit en la forma

$$e^{\lambda i}|\psi\rangle = e^{\lambda i}(a|0\rangle + b|1\rangle)$$

- Si escribimos $a$ y $b$ en forma polar, $|\psi\rangle = r_1^2 e^{\alpha_1 i}|0\rangle + r_2^2 e^{\alpha_2 i}|1\rangle$, con $r_1$ y $r_2$ números reales tales que $r_1^2 + r_2^2 = 1$. El estado de este qubit equivale al de

$$e^{-\alpha_1 i}|\psi\rangle = r_1|0\rangle + r_2 e^{(\alpha_2-\alpha_1)i}|1\rangle$$

- Por ello, queda en la siguiente forma, dependiendo sólo de 3 valores reales

$$|\psi\rangle = r_1|0\rangle + r_2 e^{\theta i}|1\rangle$$

## Esfera de Bloch

- $|\psi\rangle = r_1|0\rangle + r_2 e^{\theta i}|1\rangle$
- El valor $e^{-\alpha_1 i}$ que omitimos se denomina **fase global**
- Ejemplos

$$\begin{aligned} |0\rangle &= i \cdot |0\rangle \\ |1\rangle &= i \cdot |1\rangle \\ \sqrt{2}/2|0\rangle + i\sqrt{2}/2|1\rangle &= i\sqrt{2}/2|0\rangle - \sqrt{2}/2|1\rangle \end{aligned}$$

- La forma normal del qubit consiste en que el vector base $|0\rangle$ sólo tiene parte real, y no imaginaria (fase).

## Esfera de Bloch

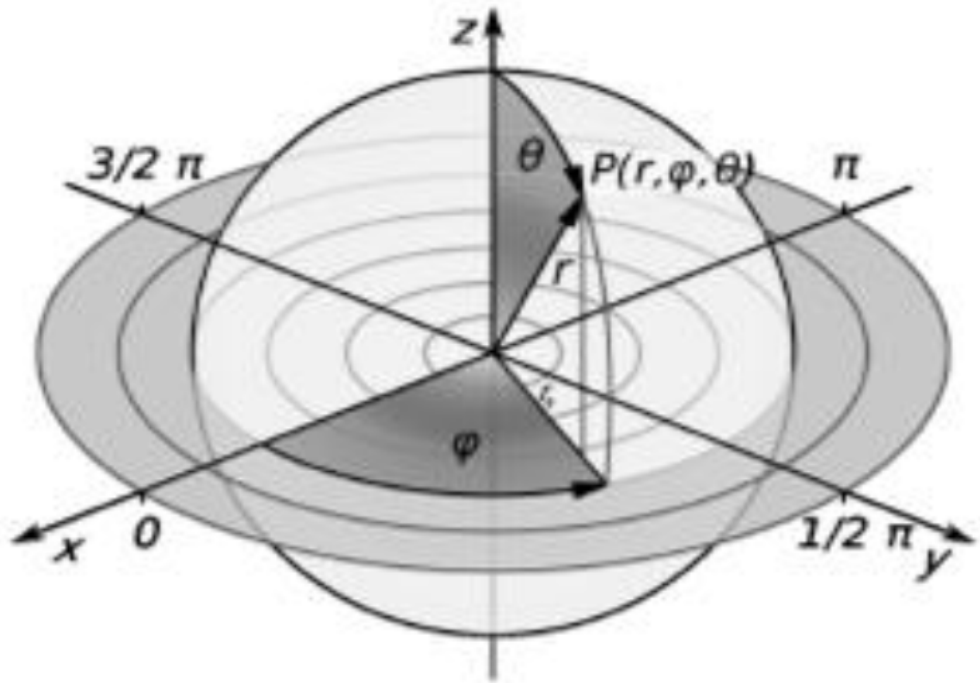
El estado de un qubit se puede representar mediante la esfera de Bloch

- ✔ El eje $Z$ tiene como unidades el valor $|0\rangle$ en el polo norte y $|1\rangle$ en el sur
- ✔ El eje $X$ tiene como unidades el valor $|+\rangle$ en el meridiano 0 con el ecuador y $|-\rangle$ en el punto contrario
- ✔ El eje $Y$ tiene como unidades el valor $|i\rangle$ en el meridiano $90^o$ con el ecuador y $|-i\rangle$ en el punto contrario
- ✔ Los vectores $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle, |i\rangle, |-i\rangle\}$ son estados puros. Cada par de ellos forman una base en el espacio de Hilbert
- ✔ Las bases más usadas son $\{|0\rangle, |1\rangle\}$ conocida como **base computacional** y $\{|+\rangle, |-\rangle\}$, como **base Hadamard**
- ✔ Es contraintuitivo el que los elementos de una base puedan estar en la misma recta y no ser ortogonales. ¡Una más!

## Esfera de Bloch

El estado de un qubit se puede representar mediante la esfera de Bloch

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

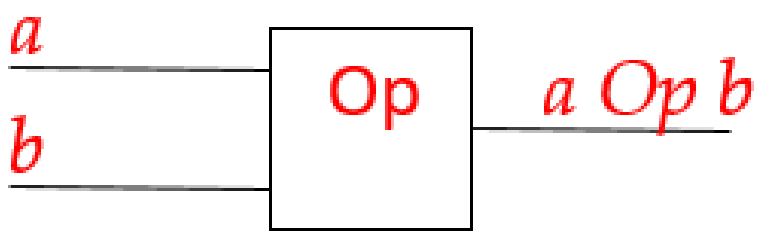


## Transformación de estados

El estado de un bit se puede transformar mediante puertas lógicas clásicas.

- ✔ Las puertas lógicas clásicas son funciones booleanas arbitrarias
- ✔ Son no reversibles

$$\text{Op} : \{0,1\} \longrightarrow \{0,1\}$$



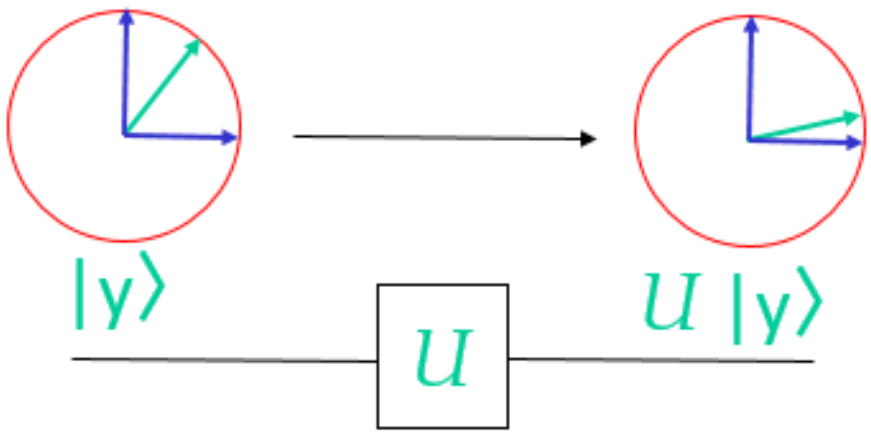

- ✔ En general:

$$\text{Op} : \{0,1\}^n \longrightarrow \{0,1\}^m$$

## Transformación de estados

El estado de un qubit se puede transformar mediante puertas lógicas cuánticas.

- ✔ Las puertas lógicas cuánticas son funciones booleanas cuánticas, donde $\mathcal{U}$ es un operador lineal representado por una matriz cuadrada
- ✔ Siempre son reversibles, y existe inverso $\mathcal{U} \cdot \mathcal{U}^{-1} = I$



## Puertas de 1 qubit

- Puerta de 1 qubit

$$|y\rangle = a\,|0\rangle + b\,|1\rangle \longrightarrow \boxed{U} \longrightarrow |y'\rangle = U\,|y\rangle$$

- Puerta NOT, o puerta X

$$Not = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$|y\rangle \longrightarrow \boxed{Not} \longrightarrow |y'\rangle = a\,|1\rangle + b\,|0\rangle$$

- Puerta Hadamard

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

$$|0\rangle \longrightarrow \boxed{H} \longrightarrow 1/\sqrt{2}\,(\,|0\rangle + |1\rangle\,)$$

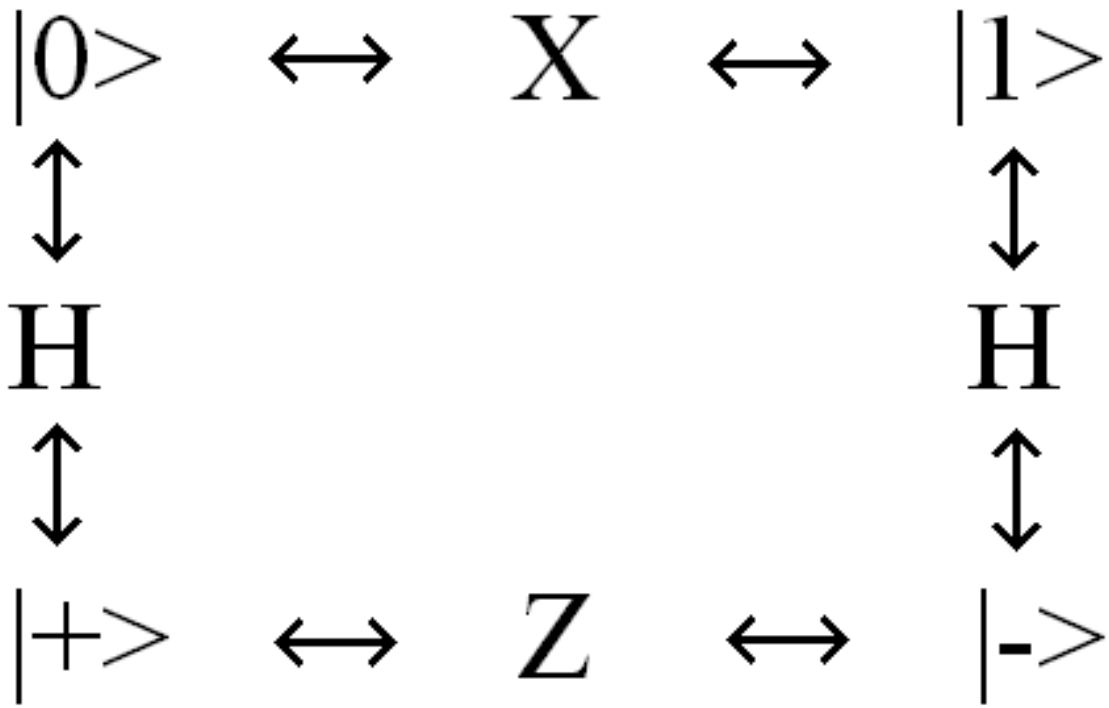
$$|1\rangle \longrightarrow \boxed{H} \longrightarrow 1/\sqrt{2}\,(\,|0\rangle - |1\rangle\,)$$

## Puertas de 1 qubit

- ✔ Puerta I (identidad). Devuelve como salida lo mismo que la entrada. Si tenemos el qubit $|y\rangle$ tenemos de salida el qubit $|y\rangle$
- ✔ Puerta X (bit flip). Equivalente a la puerta NOT. Si el qubit de entrada es $a|0\rangle + b|1\rangle$, el de salida será $b|0\rangle + a|1\rangle$. El nombre alternativo de esta puerta, bit flip, se debe a que "intercambia" (flip) los bits.
- ✔ Puerta Z (phase flip). Si el qubit de entrada es $|0\rangle$ no hace nada, pero si el que entra es un $|1\rangle$ le cambia el signo. En general, si entra un qubit $a|0\rangle + b|1\rangle$, se obtiene un qubit $a|0\rangle - b|1\rangle$.
- ✔ Puerta H (Hadamard). Convierte el qubit $|0\rangle$ en el qubit $|+\rangle$, y el qubit $|1\rangle$ en el qubit $|-\rangle$. Esta puerta es MUY importante. A primera vista lo que hace parece muy sencillo, pero tiene muchísimas aplicaciones en muchos circuitos; casi no hay ningún algoritmo cuántico que no la use. Produce la superposición de estados.

## Puertas de 1 qubit

Transformaciones



## Puertas de 1 qubit

- ✔ Puerta Y. No tiene nombre propio, pero complementa a las puertas I, X y Z en los ejes de la esfera de Bloch. Si de entrada tenemos $|0\rangle$ nos da como salida $i|1\rangle$, y con entrada $|1\rangle$ sale $-i|0\rangle$
- ✔ Puerta S (phase gate, no confundir con phase flip). Cambia $a|0\rangle + b|1\rangle$ por $a|0\rangle + bi|1\rangle$. Si se aplica dos veces seguidas la puerta S se obtiene una puerta Z
- ✔ Puerta T (puerta $\pi/4$). Cambia $a|0\rangle + b|1\rangle$ por $a|0\rangle + b\frac{1+i}{\sqrt{2}}|1\rangle$. Si se aplica dos veces se obtiene una puerta S
- ✔ Puerta R (phase shift). Cambia $a|0\rangle + b|1\rangle$ por $a|0\rangle + b\frac{\cos\theta + i\sin\theta}{\sqrt{2}}|1\rangle$, donde $\theta$ es un ángulo cualquiera que se le da externamente. Estrictamente no es una puerta, sino una colección de infinitas puertas. Puede simular tanto la puerta Z, como la S, como la T y es muy importante en la Transformada de Fourier Cuántica (QFT)
- ✔ Puerta oráculo, que describiremos normalmente como U. Es solo una notación para denotar a cualquier puerta arbitraria de un qubit

## Puertas de 1 qubit

- ✔ Puertas de Pauli

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

- ✔ Hadamard

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

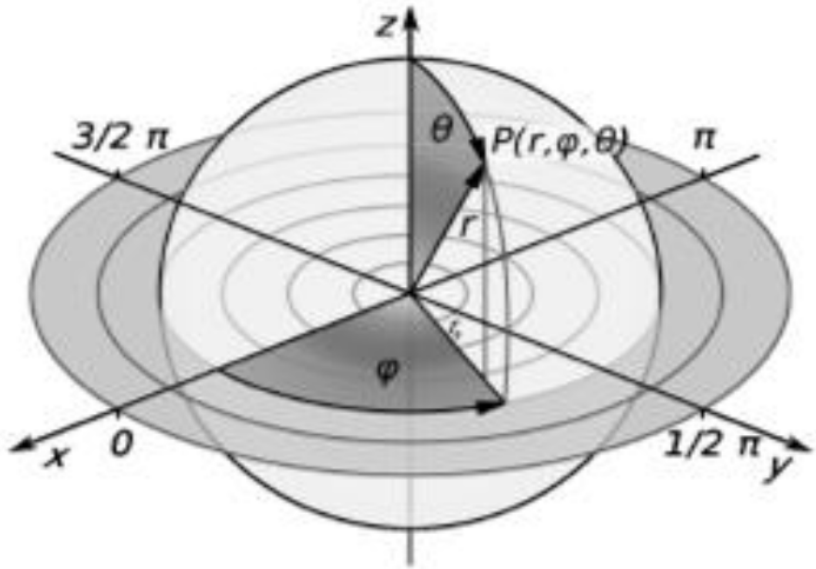
- ✔ Puerta $R_\theta$

$$R_\theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$$

- ✔ Otras

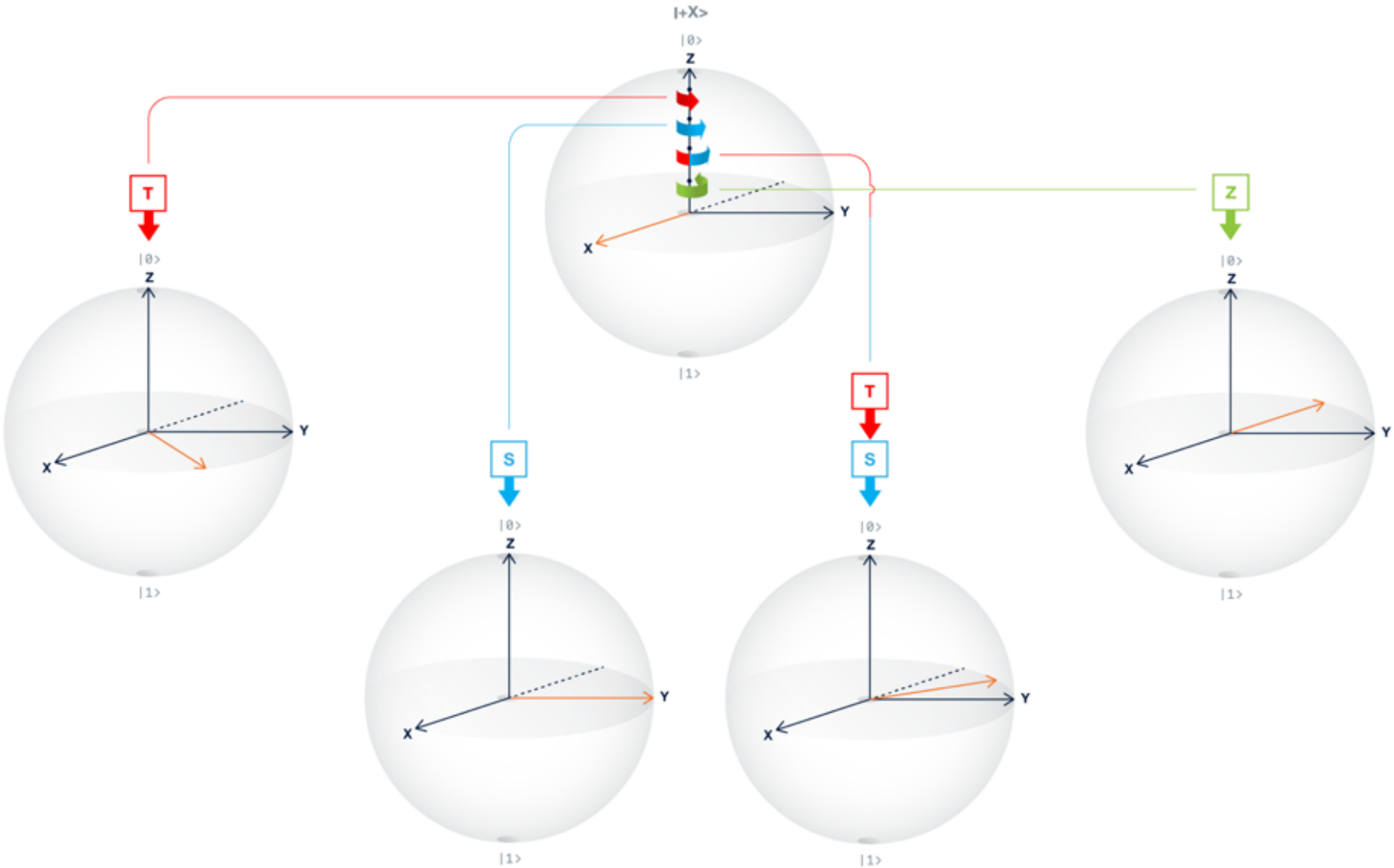
$$V = \sqrt{X} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}, \; S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, \; T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$$

## Puertas de 1 qubit




- ✔ Puertas de Pauli: Efectúan una rotación de 180º en cada uno de los 3 ejes, X, Y, Z
- ✔ Hadamard: Crea una superposición, el estado $|0\rangle$ se convierte en $|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$
- ✔ $Z(|+\rangle) = |-\rangle\,; \quad S(|+\rangle) = |i\rangle\,; \quad T(|+\rangle) = |e^{i\pi/4}\rangle$

# Puertas de 1 qubit



# Puertas de 1 qubit

| Gate sequence | Rotation around Z | Probability of 0 | Probability of 1 |
|---|---|---|---|
| H H | 0 | 1.0 | 0 |
| H T H | $\pi/4$ | 0.85 | 0.15 |
| H S H | $\pi/2$ | 0.50 | 0.50 |
| H S T H | $3\pi/4$ | 0.15 | 0.85 |
| H Z H | $\pi$ | 0 | 1 |

Create +X state | Change qubit phase | Measure in superposition basis

## Puertas de 1 qubit

- ✔ Ejemplos de rotaciones. Usamos el simulador Quirk
- ✔ Rotación en el eje X: Ver aquí
- ✔ Rotación en el eje Y: Ver aquí
- ✔ Rotación en el eje Z. Ecuador: Ver aquí
- ✔ Rotación en el eje Z. Polo Norte: Ver aquí
- ✔ Rotación en el eje Z. Polo Sur: Ver aquí

## Puertas de 1 qubit

- Un autovector de un operador lineal $A$ es un vector no nulo $|v\rangle$ tal que existe un número complejo $z$ tal que

$$A|v\rangle = z|v\rangle$$

  $z$ es conocido como autovalor
- Los vectores $|0\rangle$ y $|1\rangle$ son autovectores para el operador $Z$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} = - \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

## Puertas de 1 qubit

- ✔ Los vectores $|+\rangle$ y $|-\rangle$ son autovectores para el operador $X$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{bmatrix} = \begin{bmatrix} \sqrt{2}/2 \\ \sqrt{2}/2 \end{bmatrix}$$

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \sqrt{2}/2 \\ -\sqrt{2}/2 \end{bmatrix} = - \begin{bmatrix} \sqrt{2}/2 \\ -\sqrt{2}/2 \end{bmatrix}$$

- ✔ Los vectores $|i\rangle$ y $|-i\rangle$ son autovectores para el operador $Y$
- ✔ Los operadores de Pauli no tienen ningún efecto sobre sus autovectores

## Puertas de 1 qubit

- ✔ Ejemplos de autovectores.
- ✔ Autovector en el eje X: Ver aquí
- ✔ Autovector en el eje Y: Ver aquí
- ✔ Autovectores en ejes X e Y: Ver aquí
- ✔ Autovectores en ejes X, Y, Z: Ver aquí

## Puertas de 1 qubit

- ✔ Con las puertas de Pauli, sobre un qubit inicializado a $|0\rangle$ sólo se pueden alcanzar los estados $|0\rangle$ y $|1\rangle$
- ✔ Si añadimos la puerta H, podemos ampliar el espectro de estados alcanzables con $|+\rangle$, $|-\rangle$, $|i\rangle$ y $|-i\rangle$
- ✔ Pero sigue siendo un número muy limitado
- ✔ Con las puertas $\sqrt{X}$, S y T ampliamos el espectro un poco más
- ✔ Pero sigue siendo un número limitado

## Puertas de 1 qubit

Puerta general de rotación en el eje Z

- ✔ No es exactamente una puerta, sino una plantilla que describe un número infinito de puertas
- ✔ Puerta parametrizada $R_\varphi$, o $R_Z(\varphi)$ donde $\varphi$ es un número real, en el intervalo $[0, 2\pi)$

$$R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$$

- ✔ En particular

$$\begin{aligned} Z &= R_\pi \\ S &= R_{\pi/2} \\ T &= R_{\pi/4} \end{aligned}$$

## Puertas de 1 qubit

Puerta general de rotación en el eje Y

- ✔ También es una puerta parametrizada, o una plantilla
- ✔ Puerta $R_Y(\theta)$, donde $\theta$ es un número real, en el intervalo $[0, 2\pi)$

$$R_Y(\theta) = \begin{bmatrix} cos(\theta/2) & -sin(\theta/2) \\ sin(\theta/2) & cos(\theta/2) \end{bmatrix}$$

- ✔ En particular

$$\begin{aligned} Y &= R_Y(\pi) \\ \sqrt{Y} &= R_Y(\pi/2) \\ \sqrt{Y}|0\rangle &= H|0\rangle \end{aligned}$$

## Puertas de 1 qubit

Puerta general de rotación

- La puerta $R_\theta$ introduce una rotación generalizada en el eje $Z$
- Cualquier puerta actuando sobre un qubit se puede considerar como una rotación actuando sobre un determinado eje
- Toda rotación sobre un eje arbitrario se puede indicar mediante la posición del eje de giro, indicado por sus coordenadas respecto al eje Z con un ángulo $\varphi$, y respecto al eje $Y$ con un ángulo $\theta$. Por último, el ángulo de giro se indicará con $\lambda$
- Puerta general $U_3(\theta, \varphi, \lambda)$

$$U_3(\theta, \varphi, \lambda) = \begin{bmatrix} cos(\theta/2) & -e^{i\lambda} sin(\theta/2) \\ e^{i\varphi} sin(\theta/2) & e^{i(\lambda+\varphi)} cos(\theta/2) \end{bmatrix}$$

## Puertas de 1 qubit

- ✔ Toda puerta actuando sobre un único qubit se puede expresar como una puerta generalizada $U_3(\theta, \varphi, \lambda)$
- ✔ En particular

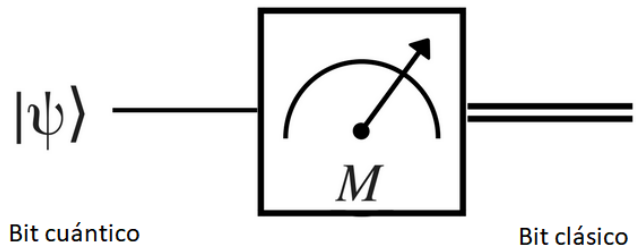
$$\begin{aligned} Z &= U_3(0, \pi, 0) \\ X &= U_3(\pi, 0, \pi) \\ Y &= U_3(\pi, \pi/2, \pi/2) \\ H &= U_3(\pi/2, 0, \pi) \end{aligned}$$

## Medida de un qubit

- ✔ Un qubit no se puede leer. En su lugar debe realizarse una medida
- ✔ La medida física consiste en, valga la redundancia, la medición del nivel energético del elemento físico donde se almacena el qubit: Átomo, ión, electrón, fotón...
- ✔ Matemáticamente, consiste en proyectar el valor del vector de la esfera de Bloch en uno de los tres ejes: X, Y o Z
- ✔ La medida estándar, que consideraremos salvo indicación contraria, será sobre el eje Z, y nos dará un valor en la base computacional $\{|0\rangle, |1\rangle\}$
- ✔ Menos habitual es la medida en el eje X, que nos dará un valor en la base Hadamard $\{|+\rangle, |-\rangle\}$. Se suele usar en algoritmos de criptografía
- ✔ También es posible una medida en el eje Y, pero es extremadamente raro

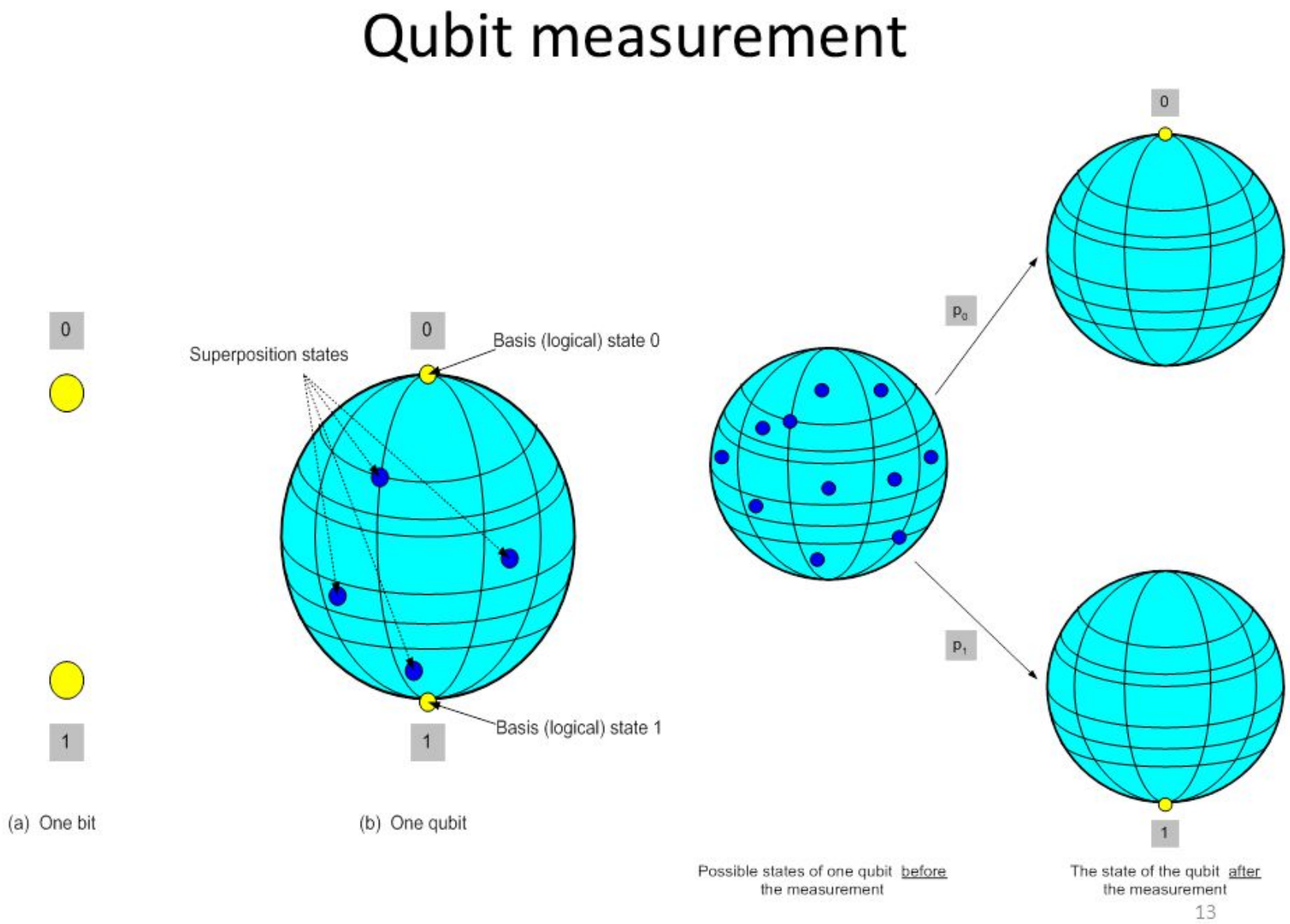
## Medida de un qubit

La medida de un qubit tiene el siguiente efecto:



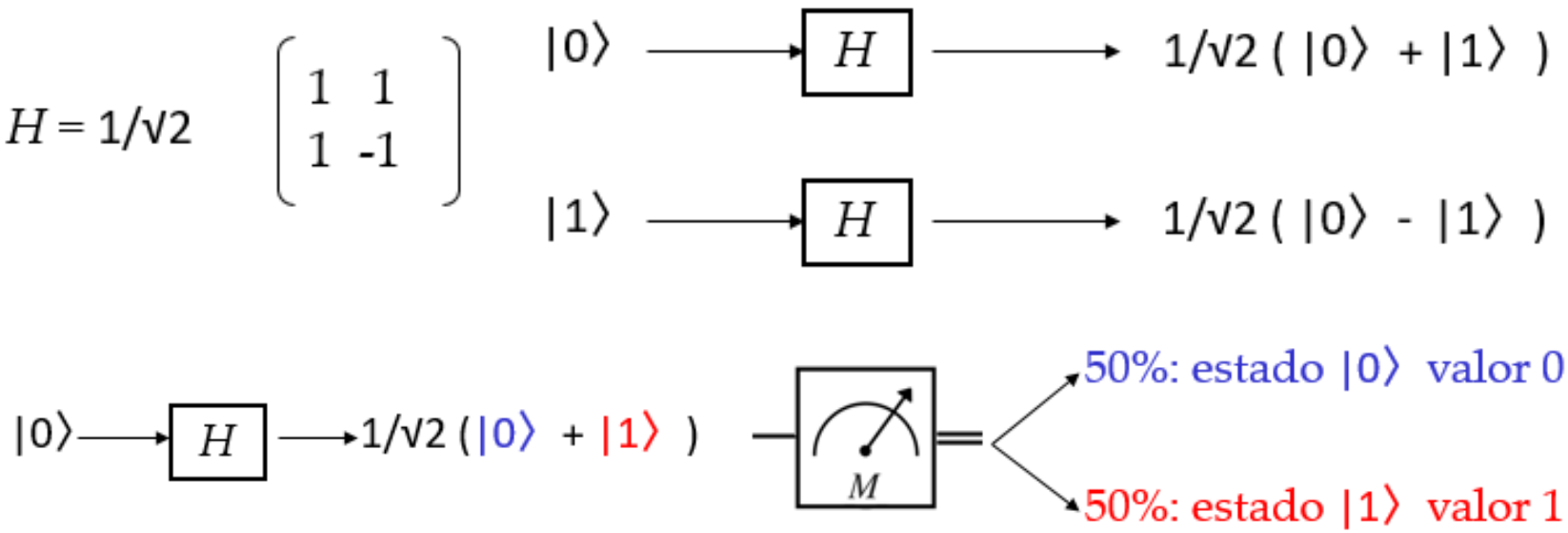

- ✔ Si el estado del qubit es $|0\rangle$ proporciona el valor 0, y el qubit continúa en el estado $|0\rangle$
- ✔ Si el estado del qubit es $|1\rangle$ proporciona el valor 1, y el qubit continúa en el estado $|1\rangle$
- ✔ Si el estado del qubit es $|y\rangle = a|0\rangle + b|1\rangle$, entonces:
  - ✗ Con probabilidad $|a|^2$ toma el valor 0, y el estado del qubit pasa a ser $|0\rangle$
  - ✗ Con probabilidad $|b|^2$ toma el valor 1, y el estado del qubit pasa a ser $|1\rangle$

# Medida de un qubit



# Medida de un qubit

Ejemplo:



## Medida de un qubit

### Definición matemática

- ✔ La probabilidad de medir un estado $|x\rangle$ en un estado $|\varphi\rangle$ la definimos como el producto interno

$$p(|x\rangle) = |\langle x|\varphi\rangle|^2$$

- ✔ La medida que hemos usado anteriormente es medir en el resultado de medir en el eje $Z$, y en concreto, medir la probabilidad de que sea el vector $|0\rangle$ el resultado de la medida.
- ✔ $1 - p(|x\rangle)$ es la probabilidad de medir el estado $|1\rangle$

$$1 - p(|x\rangle) = |\langle x|1\rangle|^2$$

## Medida de un qubit

- ✔ La medida es la proyección en un eje
- ✔ El eje está definido por un estado cuántico $|\varphi\rangle$
- ✔ El producto interno $\langle x|\varphi\rangle$ nos da un valor complejo que nos mide la amplitud de que el estado $|x\rangle$ colapse en los elementos de la base $|\varphi\rangle$ y su complementario
- ✔ El valor $|\langle x|\varphi\rangle|^2$ nos da la probabilidad de alcanzar el estado $|\varphi\rangle$

## Composición de estados

- Dados 2 qubits $|Q_1\rangle$ y $|Q_2\rangle$, podemos formar un registro de 2 qubits con el producto de Kronecker

$$|Q_1 Q_2\rangle = |Q_1\rangle \otimes |Q_2\rangle$$

- Se puede generalizar a $n$ qubits

$$|Q_1 Q_2 \dots Q_n\rangle = |Q_1\rangle \otimes |Q_2\rangle \otimes \dots |Q_n\rangle$$

- La base estándar para el espacio de Hilbert de un registro de 2 qubits es

$$\begin{aligned} |00\rangle &= |0\rangle \otimes |0\rangle \\ |01\rangle &= |0\rangle \otimes |1\rangle \\ |10\rangle &= |1\rangle \otimes |0\rangle \\ |11\rangle &= |1\rangle \otimes |1\rangle \end{aligned}$$

- Para 3 qubits es
$\{|000\rangle,\ |001\rangle,\ |010\rangle,\ |011\rangle,\ |100\rangle,\ |101\rangle,\ |110\rangle,\ |111\rangle\}$

## Composición de estados

- ✔ Registro general de $n$ qubits

$$|\psi\rangle = \sum_{0 \leq x < 2^n} \alpha_x |x\rangle, \quad \sum_{0 \leq x < 2^n} |\alpha_x|^2 = 1$$

- ✔ Requiere $2^n$ números complejos. P.e. para 3 qubits

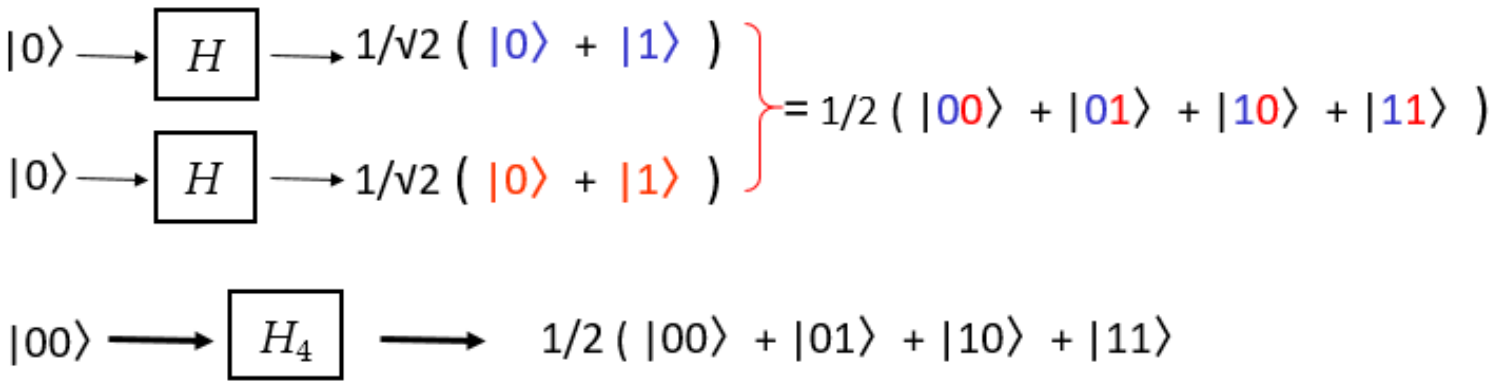
$$\begin{aligned} |\psi\rangle \quad = \quad & \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{011}|011\rangle + \\ & \alpha_{100}|100\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle \end{aligned}$$

Con

$$\begin{aligned} & |\alpha_{000}|^2 + \alpha_{001}|^2 + |\alpha_{010}|^2 + |\alpha_{011}|^2 + \\ & |\alpha_{100}|^2 + |\alpha_{101}|^2 + |\alpha_{110}|^2 + |\alpha_{111}|^2 \ = \ 1 \end{aligned}$$

## Puertas de 2 qubits

- Puerta de Hadamard de 2 qubits




- Donde la puerta $H_4$ es la matriz $4 \times 4$

$$H_4 = H \otimes H = \frac{1}{2} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

## Composición de estados

- ✔ Ejemplos de composición de estados
- ✔ Registro de 2 qubits: Ver aquí
- ✔ Registro de 3 qubits: Ver aquí
- ✔ Registro de 4 qubits: Ver aquí
- ✔ Registro de 8 qubits: Ver aquí
- ✔ Registro de 10 qubits: Ver aquí
- ✔ Registro de 16 qubits: Ver aquí

## Composición de estados

- ✔ Podemos definir también la matriz de densidad de un registro de qubits $|\psi\rangle\langle\psi|$

$$|\psi\rangle\langle\psi| = |\psi\rangle \otimes \langle\psi|$$

- ✔ En un registro de 2 qubits con $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$

$$|\psi\rangle\langle\psi| = \begin{pmatrix} |a|^2 & ab^\dagger & ac^\dagger & ad^\dagger \\ ba^\dagger & |b|^2 & bc^\dagger & bd^\dagger \\ ca^\dagger & cb^\dagger & |c|^2 & cd^\dagger \\ da^\dagger & db^\dagger & dc^\dagger & |d|^2 \end{pmatrix}$$

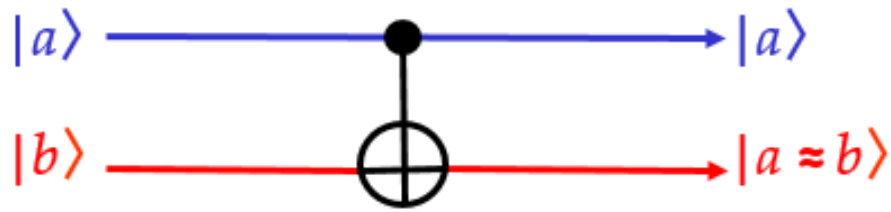
## Composición de estados

- ✔ Ejemplos. Matriz de densidad
- ✔ Registro de 2 qubits: Ver aquí
- ✔ Registro de 3 qubits: Ver aquí
- ✔ Registro de 4 qubits: Ver aquí
- ✔ Registro de 6 qubits: Ver aquí
- ✔ Registro de 8 qubits: Ver aquí

## Puerta CNot

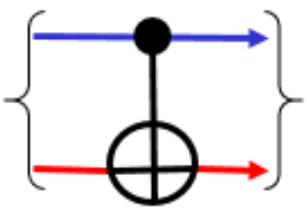
- ✔ Puerta Not Controlado, CNot
- ✔ Puerta del conjunto universal

$CNot$:



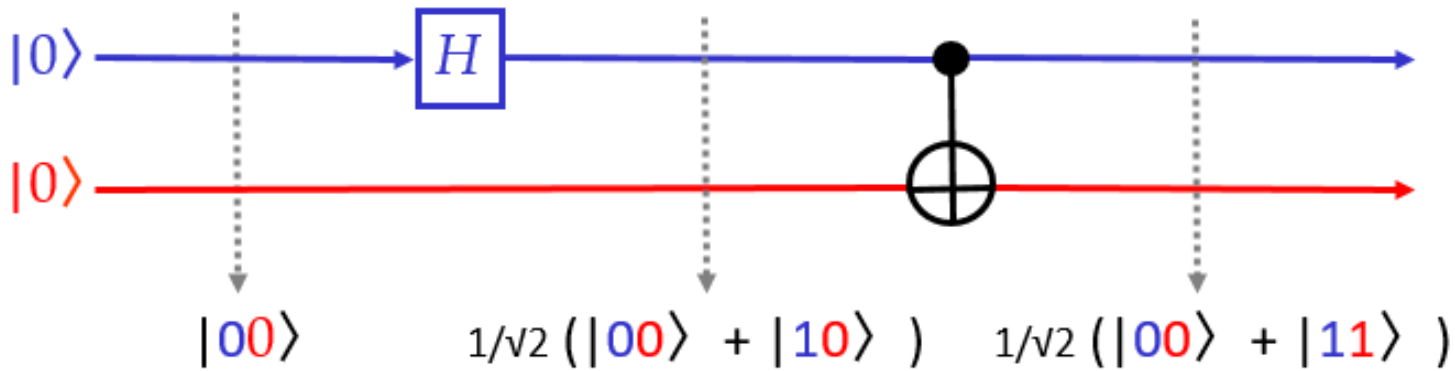

$$CNot\,(|00\rangle) = |00\rangle$$
$$CNot\,(|01\rangle) = |01\rangle$$
$$CNot\,(|10\rangle) = |11\rangle$$
$$CNot\,(|11\rangle) = |10\rangle$$

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

$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$  $a|00\rangle + b|01\rangle + c|11\rangle + d|10\rangle$

## Puertas de 2 qubits

- ✔ Estados entrelazados, par EPR o par de Bell




- ✔ Tras la ejecución del operador, los dos qubits están entrelazados. Forman un estado EPR. Si uno de ellos es $|0\rangle$, el otro también, y viceversa con $|1\rangle$.

## Estados entrelazados

- Un par entrelazado forma un estado inalcanzable por composición de estados de qubits
- Sea $|y\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$
- Supongamos dos qubits $A$ y $B$ tales que su composición es $y$

$$\begin{aligned} |A\rangle &= a_1|0\rangle + b_1|1\rangle \\ |B\rangle &= a_2|0\rangle + b_2|1\rangle \end{aligned}$$

Pero $|AB\rangle = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$

- Sin embargo, el sistema

$$\begin{aligned} a_1a_2 &= \frac{1}{\sqrt{2}} \\ a_1b_2 &= 0 \\ b_1a_2 &= 0 \\ b_1b_2 &= \frac{1}{\sqrt{2}} \end{aligned}$$

no tiene solución

## Puertas de n qubits

- ✔ Dado un registro $|\psi\rangle$ de $n$ qubits
- ✔ Se puede obtener una puerta de $n$ entradas como composición de puertas de 1 qubit en la forma

$$U = U_1 \otimes U_2 \otimes \ldots \otimes U_n$$

- ✔ O bien se puede obtener como composición de puertas de 1 qubit y puertas CNot de 2 qubits
- ✔ Ejemplo. 3 puertas de 1 qubit. Ver aquí
- ✔ Ejemplo. 3 puertas de 1 qubit, y un estado de Bell. Ver aquí

## Criptografía cuántica

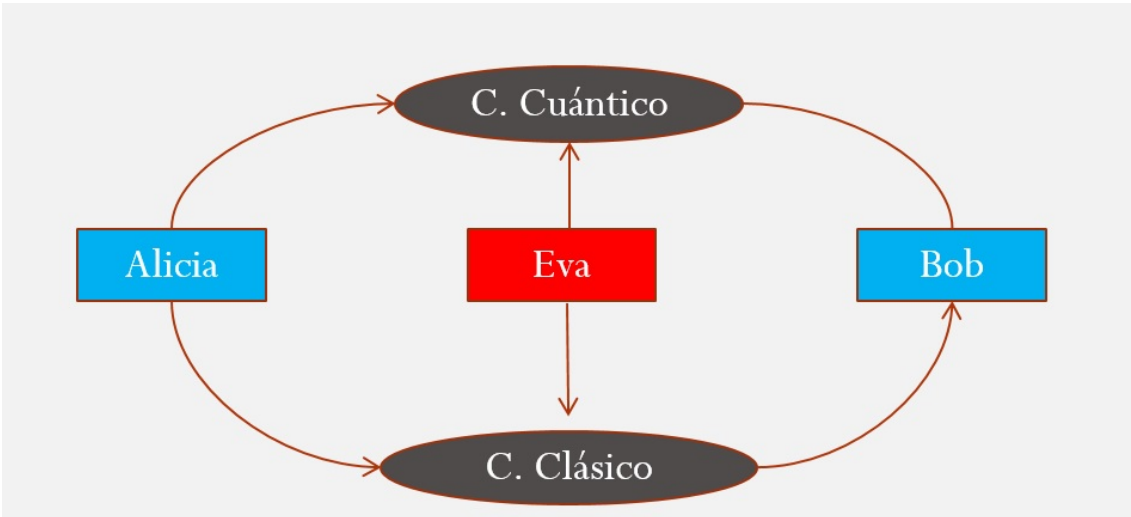
- ✔ La criptografía cuántica utiliza principios de la física cuántica para garantizar la confidencialidad en la transmisión de la información
- ✔ Una de las propiedades más importantes de la criptografía cuántica es que si se intenta espiar durante la transmisión, el proceso altera el resultado
- ✔ Esto es consecuencia del teorema de no clonado
- ✔ La seguridad de la criptografía cuántica descansa en las bases de la mecánica cuántica, a diferencia de la criptografía tradicional que descansa en supuestos de complejidad computacional

## Criptografía cuántica

- ✔ Uno de los problemas de mayor dificultad para una comunicación segura mediante un sistema de clave privada es la distribución y almacenamiento de las claves
- ✔ Shannon, en 1949, establece que si la clave es aleatoria, de la misma longitud que el mensaje a cifrar y se usa una única vez, el cifrado es seguro
- ✔ Sin embargo, la necesidad de distribuir y almacenar de manera segura las claves, en general largas y de un solo uso, limita las posibilidades de este sistema

# Criptografía cuántica

- ✔ Existen diferentes protocolos cuánticos de distribución de claves denominados QKD (Quantum Key Distribution), ideados con el fin de intercambiar claves privadas de un solo uso, que se pueden usar en sistemas simétricos de seguridad.
- ✔ De hecho, la llamada criptografía cuántica es la primera aplicación comercial de la mecánica cuántica.



## Protocolo BB84

- ✔ Propuesto por Brassard y Bennet en 1984
- ✔ Se usan fotones polarizados enviados entre el emisor (Alice) y el receptor (Bob) mediante un canal cuántico, por ejemplo, una fibra óptica
- ✔ También se necesita la existencia de un canal público (no necesariamente cuántico) entre Alice y Bob, como por ejemplo Internet u ondas de radio, el cual se usa para mandar información requerida para la construcción la clave secreta compartida
- ✔ Ninguno de los canales necesita ser seguro, es decir, se asume que un intruso (de nombre Eve) puede intervenirlos con el fin de obtener información

## Protocolo BB84

- ✔ Alice y Bob pretenden intercambiar una calve de forma segura, y disponen de los dos canales de comunicación indicados, clásico y cuántico
- ✔ Eva tiene acceso a las comunicaciones, que no son seguras
- ✔ Cada qubit puede ser implementado por un simple fotón, que puede ser transmitido por medio de un dispositivo óptico, incluso usando satélites
- ✔ Cada qubit (fotón) podrá estar en uno de cuatro estados posibles
- ✔ El protocolo ha sido llevado a la práctica

## Protocolo BB84

- ✔ En primer lugar, Alice debe preparar un sistema de $n$ qubits. No es necesario que estén entrelazados, por lo que $n$ puede ser arbitrariamente grande
- ✔ La idea fundamental es que Alice preparará los qubits por medio de un doble sistema
- ✔ En primer lugar, codificará los qubits mediante los estados cuánticos $|0\rangle$ y $|1\rangle$. Pero además, estos estados podrán estar codificados en base computacional o Hadamard, siendo en este caso los estados posibles $|+\rangle$ para el bit 0, y $|-\rangle$ para el bit 1

## Protocolo BB84

- ✔ Los estados posibles pueden ser $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$
- ✔ Pueden ser medidos con base computacional ($B_c$) o Hadamard ($B_H$)

| Estado | Medido con $B_c$ | Medido con $B_H$ |
|---|---|---|
| $\|0\rangle$ | $\|0\rangle$ con $p = 1$ | $\|+\rangle$ con $p = 1/2$<br>$\|-\rangle$ con $p = 1/2$ |
| $\|1\rangle$ | $\|1\rangle$ con $p = 1$ | $\|+\rangle$ con $p = 1/2$<br>$\|-\rangle$ con $p = 1/2$ |
| $\|+\rangle$ | $\|0\rangle$ con $p = 1/2$<br>$\|1\rangle$ con $p = 1/2$ | $\|+\rangle$ con $p = 1$ |
| $\|-\rangle$ | $\|0\rangle$ con $p = 1/2$<br>$\|1\rangle$ con $p = 1/2$ | $\|-\rangle$ con $p = 1$ |

## Protocolo BB84

- El protocolo BB84, propuesto en 1984 por Bennet y Brassard sigue los siguientes pasos
- **Paso 1**. Alice genera una cadena aleatoria de ceros y unos
- **Paso 2**. Para cada qubit, Alice elige aleatoriamente una base $B_c$ o $B_H$ y envía a Bob el qubit codificado, en uno de los 4 estados posibles
- **Paso 3**. Bob recibe la cadena de qubits, y realiza una medida de cada uno de ellos, eligiendo en cada caso una base al azar
- **Paso 4**. Reconcialiación de claves. Bob comunica, por un canal clásico, la cadena de bits que ha usado para la medida, y Alice responde por el mismo canal cuales son coincidentes
- **Paso 5**. Clave bruta. Para aquellos qubits de base coincidente, Bob y Alice disponen de una clave compartida

## Protocolo BB84

### Ejemplo

| Mensaje | 0 | 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Base Alice | $B_c$ | $B_H$ | $B_c$ | $B_H$ | $B_c$ | $B_H$ | $B_c$ | $B_c$ | $B_H$ | $B_H$ |
| Codificación | $\|0\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|+\rangle$ | $\|1\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| Base Bob | $B_c$ | $B_c$ | $B_H$ | $B_H$ | $B_H$ | $B_c$ | $B_c$ | $B_c$ | $B_H$ | $B_H$ |
| Medida Bob | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|-\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|-\rangle$ |
| Reconciliación | 0 | | | 0 | | | 0 | 0 | 0 | 1 |

La clave 000001 es secreta

## Protocolo BB84

### Seguridad

- ✔ Eva puede interceptar los qubits y medirlos
- ✔ Eso implica que el qubit puede cambiar su estado, si no se mide en en la misma base en que se codificó por Alice
- ✔ La probabilidad de que la base elegida no sea la correcta es $1/2$, y la probabilidad de que de el valor equivado es $1/2$. Por tanto, con probabilidad $1/4$ el qubit cambiará de valor
- ✔ Alice y Bob pueden compartir un fragmento de la clave. Por ejemplo, los 10 primeros
- ✔ En ausencia de ruido, la probabilidad de que todos los bits coincidan si la clave ha sido atacada es $(3/4)^{10}$, es decir un 5 %
- ✔ Con un número suficiente de bits de intercambio para contraste, se puede garantizar que la transmisión no ha sido interceptada

## Protocolo B92

- ✔ Propuesto por Bennet en 1992
- ✔ Es muy parecido a BB84, más simplificado
- ✔ Se usan fotones polarizados enviados entre el emisor (Alice) y el receptor (Bob) mediante un canal cuántico, por ejemplo, una fibra óptica
- ✔ También se necesita la existencia de un canal público (no necesariamente cuántico) entre Alice y Bob, como por ejemplo Internet u ondas de radio, el cual se usa para mandar información requerida para la construcción la clave secreta compartida
- ✔ Ninguno de los canales necesita ser seguro, es decir, se asume que un intruso (de nombre Eve) puede intervenirlos con el fin de obtener información

## Protocolo B92

- ✔ En primer lugar, Alice debe preparar un sistema de $n$ qubits. No es necesario que estén entrelazados, por lo que $n$ puede ser arbitrariamente grande
- ✔ En este caso, Alice preparará los qubits por medio de un sistema simple
- ✔ Para ello, genera una secuencia de bits $a$, cada uno de ellos puede estar en 0 o en 1
- ✔ Después, codificará los qubits mediante los estados cuánticos $|0\rangle$ y $|+\rangle$. En el primer caso, si el bit $a$ está a 0, y en el segundo si está a 1
- ✔ Los qubits se envían por el canal cuántico

## Protocolo B92

- Por su parte, Bob genera una secuencia de bits $b$, cada uno de ellos puede estar en 0 o en 1
- Cuando recibe los qubits por el canal cuántico, realiza una medida de cada uno de ellos. Si el bit $b$ está a 0 la medida se hace en base computacional C, si está a 1 se hace en base Hadamard H
- Bob publica los resultados de las medidas por el canal clásico, pero sólo para los qubits con medida 1

## Protocolo B92

- ✔ Esto es por lo siguiente
- ✔ Alice ha codificado siempre un 0, bien en base Computacional si el bit $a$ es 0 o Hadamard, si es 1
- ✔ Al medir Bob, si la base es coincidente siempre medirá 0
- ✔ Si la base no es coincidente, con probabilidad $1/2$ medirá 0 o 1

| Estado | Medido con $B_c$ | Medido con $B_H$ |
|---|---|---|
| $\|0\rangle$ | 0 con $p = 1$ | 0 con $p = 1/2$<br>1 con $p = 1/2$ |
| $\|+\rangle$ | 0 con $p = 1/2$<br>1 con $p = 1/2$ | 0 con $p = 1$ |

## Protocolo B92

- ✔ Por tanto, si la medida es 0, Bob no puede saber en qué base fue codificado el qubit
- ✔ Puede ser porque Alice codificó 0 en la misma base, o porque lo codificó en base contraria, y la medida ha salido con 1/2 de probabilidad
- ✔ PERO si la medida es 1, forzosamente Alice lo condificó con base contraria, y se ha medido 1 con probabilidad 1/2
- ✔ Bob conoce su base, por lo que conoce también la de Alice, que es la contraria

## Protocolo B92

### Ejemplo

| Mensaje | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Codificación | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ |
| Cadena de Bob | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| Base Bob | $B_C$ | $B_H$ | $B_H$ | $B_H$ | $B_H$ | $B_C$ | $B_C$ | $B_C$ | $B_H$ | $B_H$ |
| Medida Bob | 0 | ? | 0 | ? | 0 | ? | ? | 0 | ? | 0 |

## Protocolo B92

### Ejemplo

| Mensaje | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 |
|---|---|---|---|---|---|---|---|---|---|---|
| Codificación | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|+\rangle$ | $\|0\rangle$ | $\|0\rangle$ | $\|+\rangle$ |
| Cadena de Bob | 0 | 1 | 1 | 1 | 1 | 0 | 0 | 0 | 1 | 1 |
| Base Bob | $B_C$ | $B_H$ | $B_H$ | $B_H$ | $B_H$ | $B_C$ | $B_C$ | $B_C$ | $B_H$ | $B_H$ |
| Medida Bob | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| Reconciliación | | 0 | | | | 1 | | | 0 | |

La clave 010 es secreta

## Protocolo B92

### Seguridad

- ✔ Es similar a la de BB84
- ✔ Una medida interceptada por Eva alterará el resultado
- ✔ Puede ser detectada compartiendo un fragmento de la clave común compartida

# Criptografía cuántica

## Comparación

- ✔ El rendimiento de BB84 es superior a B92. En el primero, la clave bruta es aproximadamente del 50 % de los bits, en el segundo es del 25 %
- ✔ La codificación de BB84 precisa 4 posibles estados cuánticos para los qubits, la de B92 solo necesita de 2
- ✔ Los errores también deben ser tenidos en cuenta, no sólo la posibilidad de intercepción, porque los estados cuánticos pueden decaer (decoherencia)
- ✔ El uso de menos estados cuánticos, hace que la posibilidad de errores de B92 sea menor

## Criptografía cuántica

- ✔ En 2010 se publicó la transmisión de clave común cuántica en 300 km de distancia
- ✔ Se utilizó un protocolo de estados entrelazados, en lugar de BB84 o B91

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG IOP Institute of Physics

OPEN ACCESS

Feasibility of 300 km quantum key distribution with entangled states

To cite this article: Thomas Scheidl *et al* 2009 *New J. Phys.* **11** 085002

View the article online for updates and enhancements.

## Casos de éxito

Entre los algoritmos cuánticos que hasta ahora han tenido mayor repercusión encontramos:

- ✔ Algoritmo de Deutsch. Dada una función de la que sabemos que es constante o balanceada, decidir cual de las dos es.
  El algoritmo determinista tiene un coste exponencial en el tamaño en bits del input. El algoritmo cuántico lo hace en tiempo constante.
- ✔ Algoritmo de Grover. Dada una lista no ordenada de valores enteros, y otro determinado dato, decidir si dicho dato está o no en la lista.
  El algoritmo determinista tiene un coste $\mathcal{O}(n)$, busca todos los elementos si no está. El algoritmo cuántico lo hace en tiempo $\mathcal{O}(\sqrt{n})$
- ✔ Algoritmo de Shor. Descompone un número $n$ en sus factores primos.
  El algoritmo determinista, basado en la criba de Eratóstenes tiene un tiempo $\mathcal{O}(\sqrt{n})$. El algoritmo cuántico lo hace en $\mathcal{O}(\log^3 N)$.
  Este último resultado es de importancia fundamental en seguridad informática y criptografía.

## Simulador Quirk

**Simulador gráfico de uso muy sencillo**

- ✔ On line desde el navegador de internet
- ✔ Se trata de IBM Quantum Experience
- ✔ Totalmente gráfico
- ✔ Hasta 16 qubits. Si bien por encima de 10 se vuelve engorroso
- ✔ Se observa completamente el funcionamiento

## Simulador Quirk

**Enlace:** El enlace directo es https://algassert.com/quirk

## Simulador Quirk

### Evaluación de funciones booleanas

- ✔ Supongamos una fórmula de 4 variables booleanas $\{x_0, x_1, x_2, x_3\}$
- ✔ La fórmula está en forma normal conjuntiva, es decir una conjunción de varias disyunciones (negadas o no)
- ✔ Ejemplo

$$f(x_0, x_1, x_2, x_3) = (x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

## Simulador Quirk

### Evaluación de funciones booleanas

$$f(x_0, x_1, x_2, x_3) = (x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

Evaluación con la tabla de la verdad

| N | x0 | x1 | x2 | x3 | c1 | c2 | c3 | c4 | fórmula |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 0 |
| 2 | 1 | 0 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 3 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 | 0 |
| 4 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 |
| 5 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 6 | 1 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 7 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| 8 | 1 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 |
| 9 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 |
| 10 | 1 | 0 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 11 | 0 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 12 | 1 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 |
| 13 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 |
| 14 | 1 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 15 | 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 16 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

## Simulador Quirk

$$(x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

- ✔ Cada variable se codifica con un qubit, inicializada con una puerta Hadamard
- ✔ Cada cláusula se codifica con un qubit, inicializado a $|0\rangle$
- ✔ La fórmula global se codifica con un qubit, inicializado a $|0\rangle$

**Enlace:** Click aquí

## Simulador Quirk

Cláusula: $(x_0 \vee x_1 \vee \neg x_3)$

- ✔ Cada variable se codifica con un control o anticontrol, dependiendo de si está negada o no
- ✔ Los controles actúan sobre el qubit de la cláusula, que está negado previamente

**Enlace:** Click aquí

## Simulador Quirk

$$(x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

- ✔ Se codifican todas las cláusulas
- ✔ La fórmula global se codifica con un qubit, inicializado a $|0\rangle$

**Enlace:** Click aquí

## Simulador Quirk

$$(x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

✔ La fórmula global es la conjunción de todas las cláusulas

**Enlace:** Click aquí

## Simulador Quirk

$$(x_0 \vee x_1 \vee \neg x_3) \wedge (\neg x_0 \vee x_2 \vee x_3) \wedge (x_2 \vee x_3) \wedge (x_0 \vee \neg x_1 \vee x_3)$$

- ✔ La fórmula global es la conjunción de todas las cláusulas
- ✔ **Importante.** Tras la codificación es necesario **descomputar** las cláusulas. Por razones técnicas

**Enlace:** Click aquí

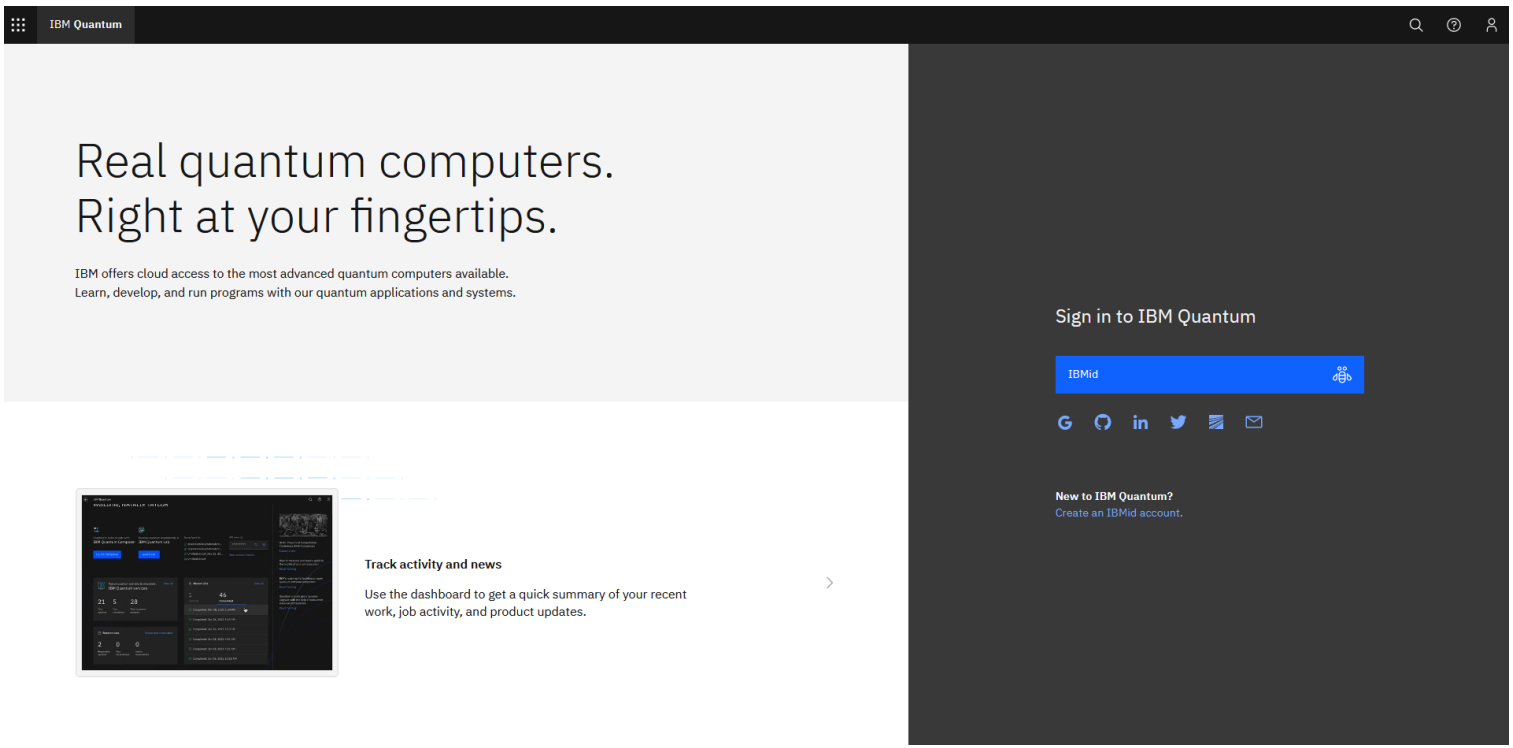
# IBM Quantum Experience

## Primer programa cuántico

- ✔ Usaremos un computador real accesible por Internet
- ✔ Se trata de IBM Quantum Experience
- ✔ Primer computador cuántico comercial, presentado en 2019
- ✔ En la actualidad disponde de varios computadores accesibles. Los de 5 qubits son gratuitos
- ✔ Cuales están disponibles dependen del momento de acceso

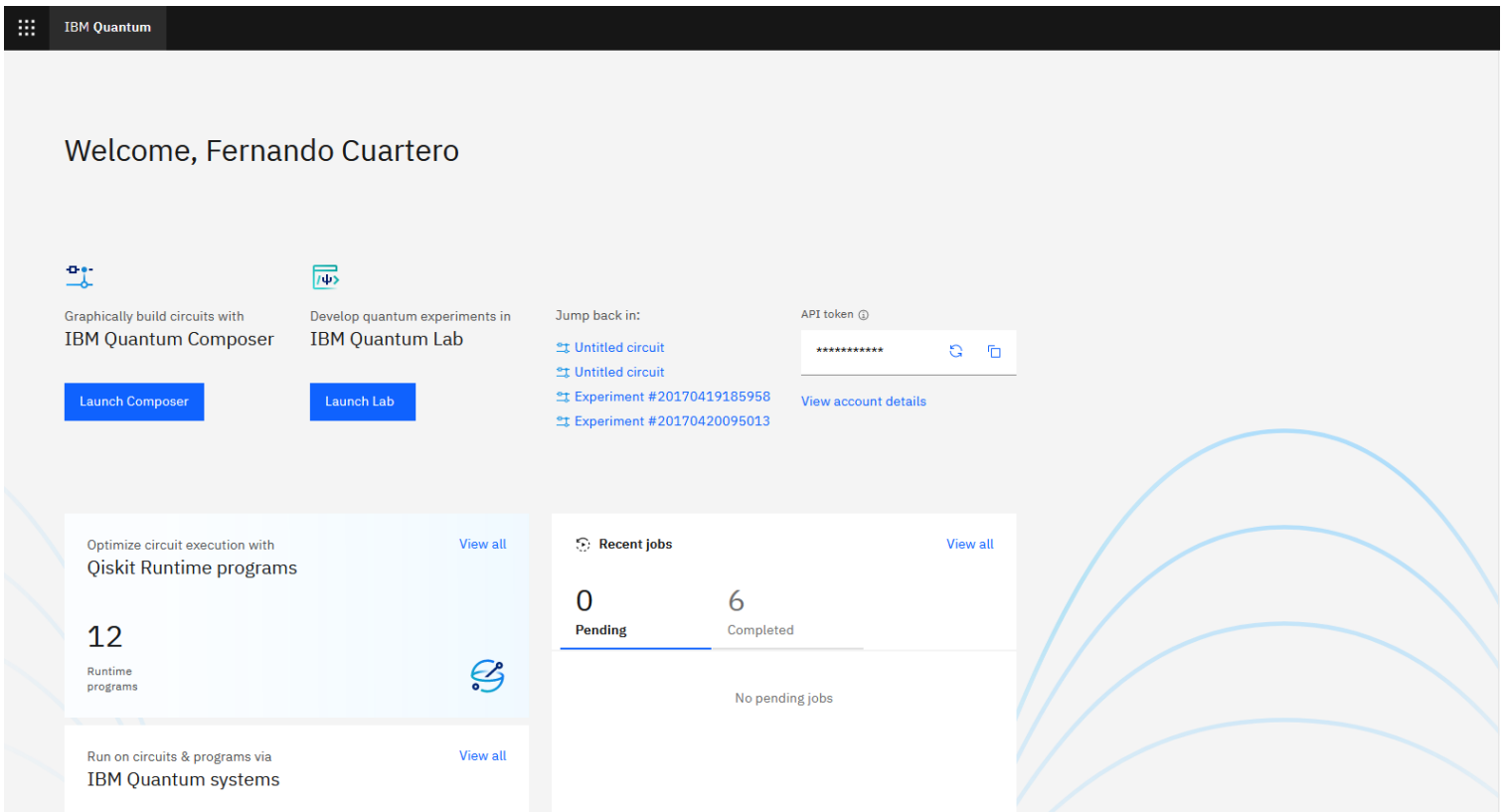
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



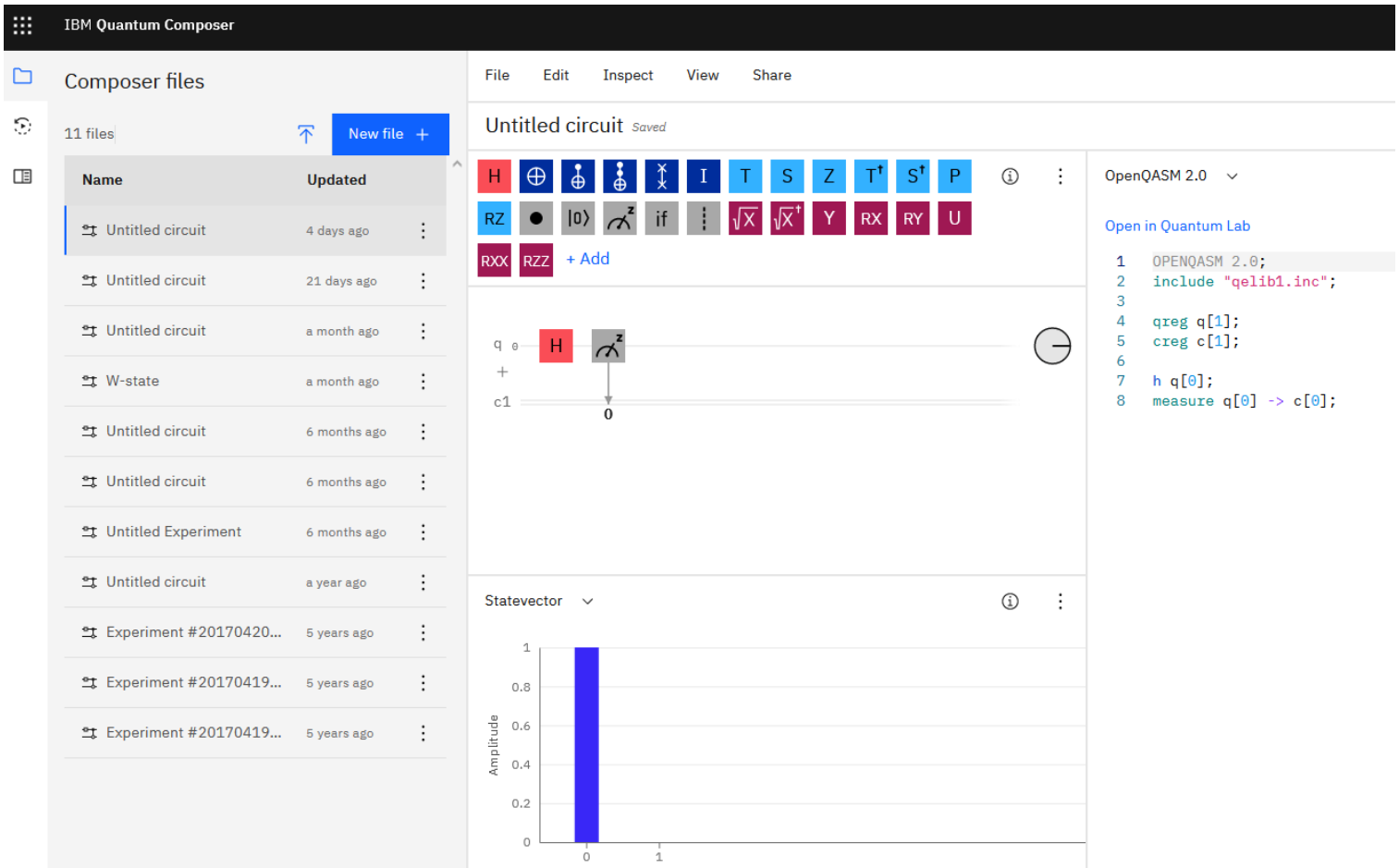
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



## IBM Quantum Experience

- ✔ Texto del programa nuevo

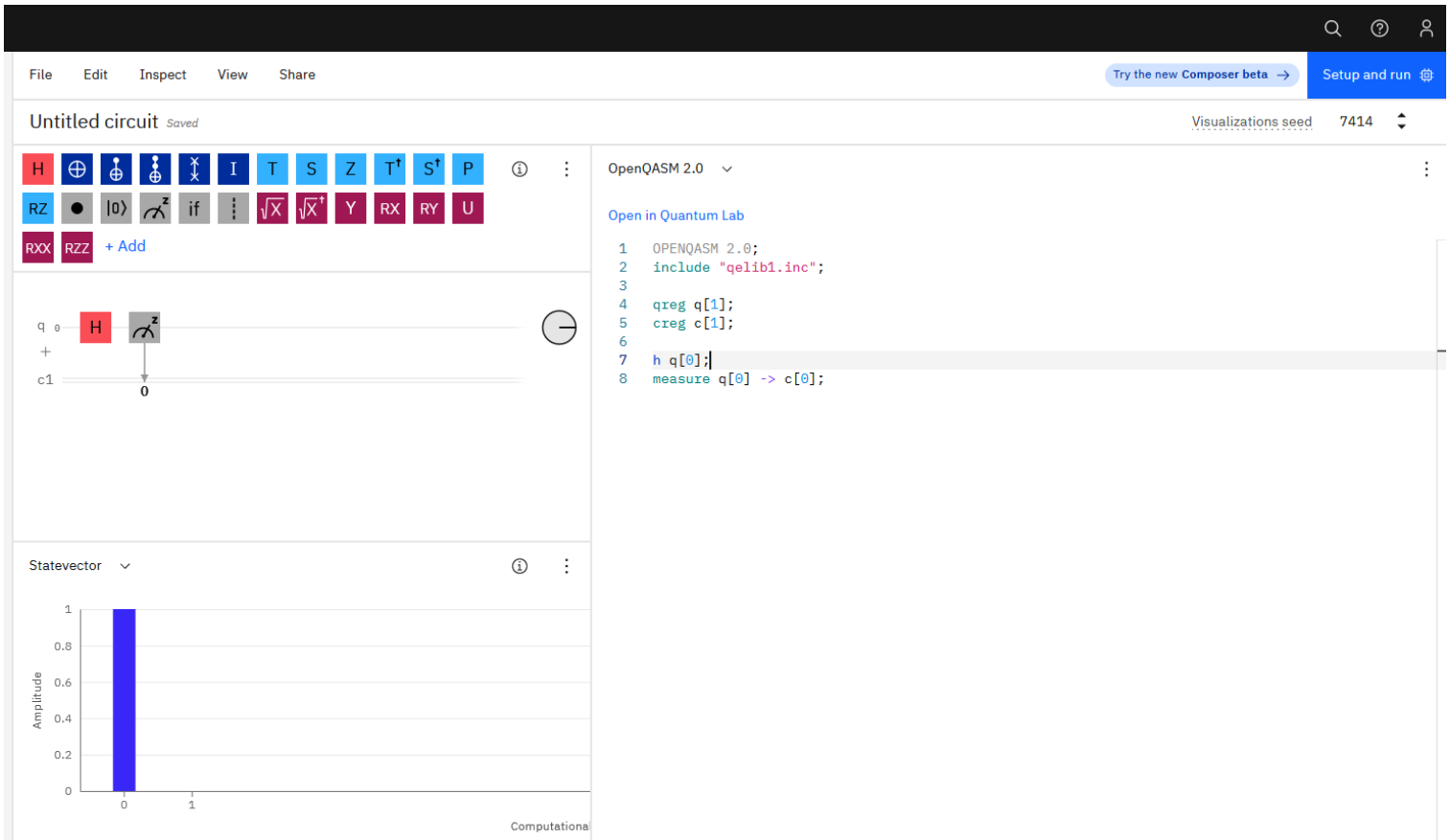
```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[3];
creg c[3];
```

- ✔ Texto que debe aparecer

```
OPENQASM 2.0;
include "qelib1.inc";
qreg q[1];
creg c[1];
h q[0];
measure q[0] - > c[0];
```

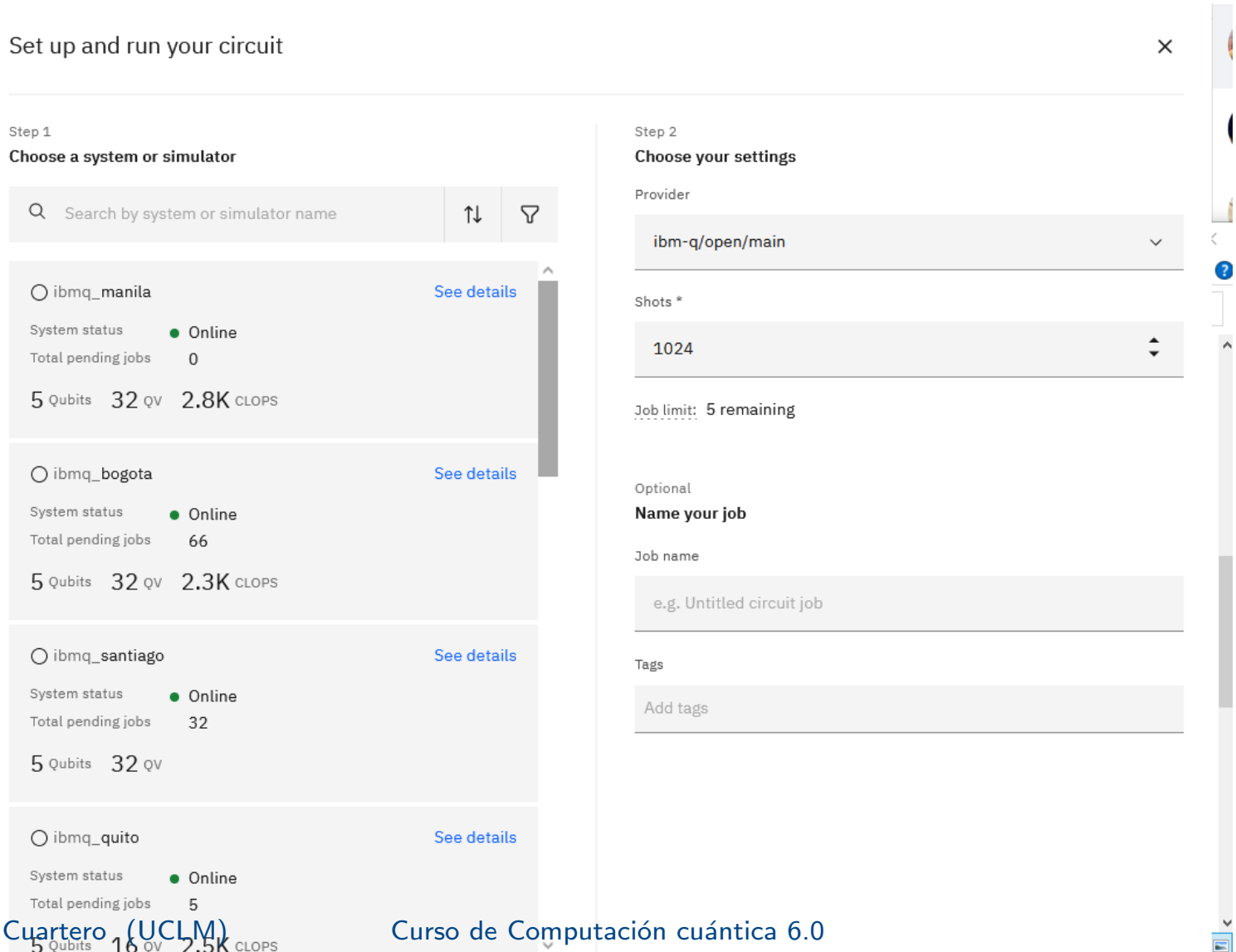
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



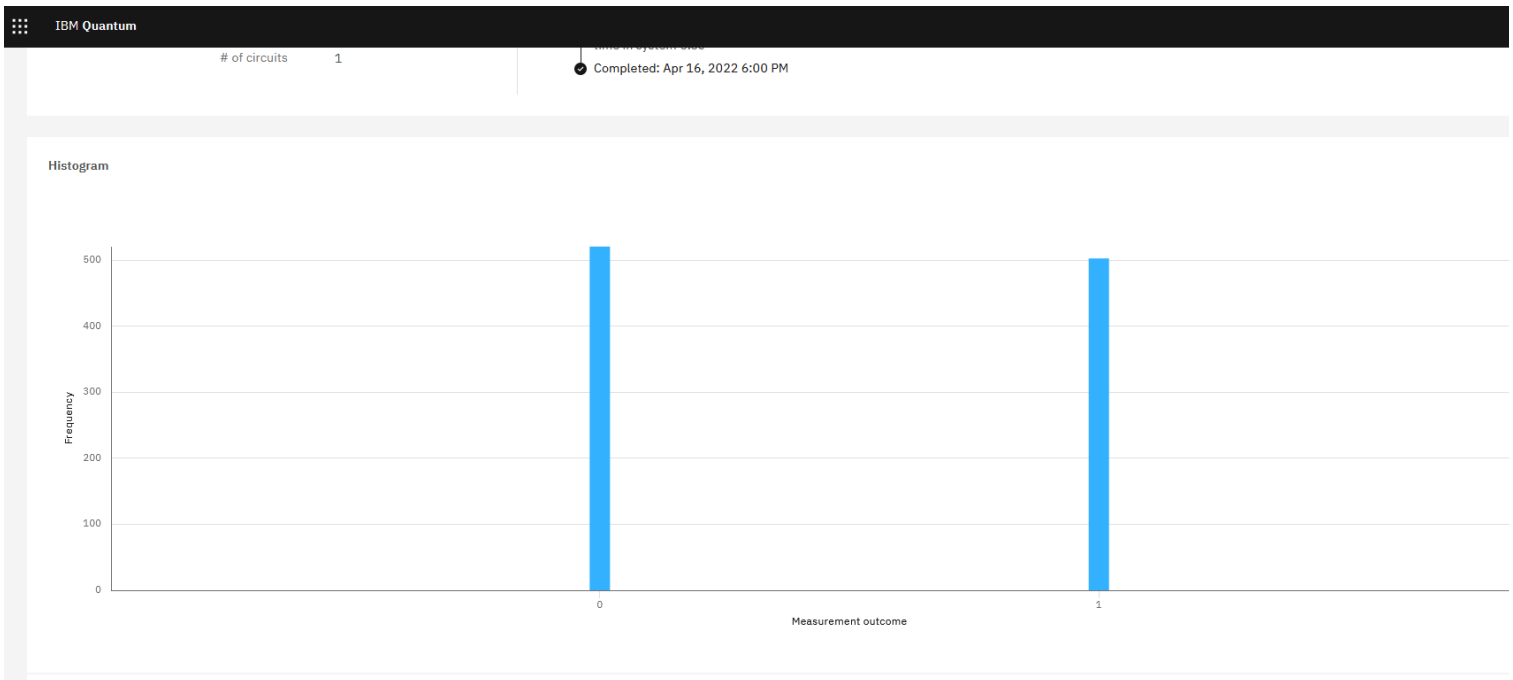
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



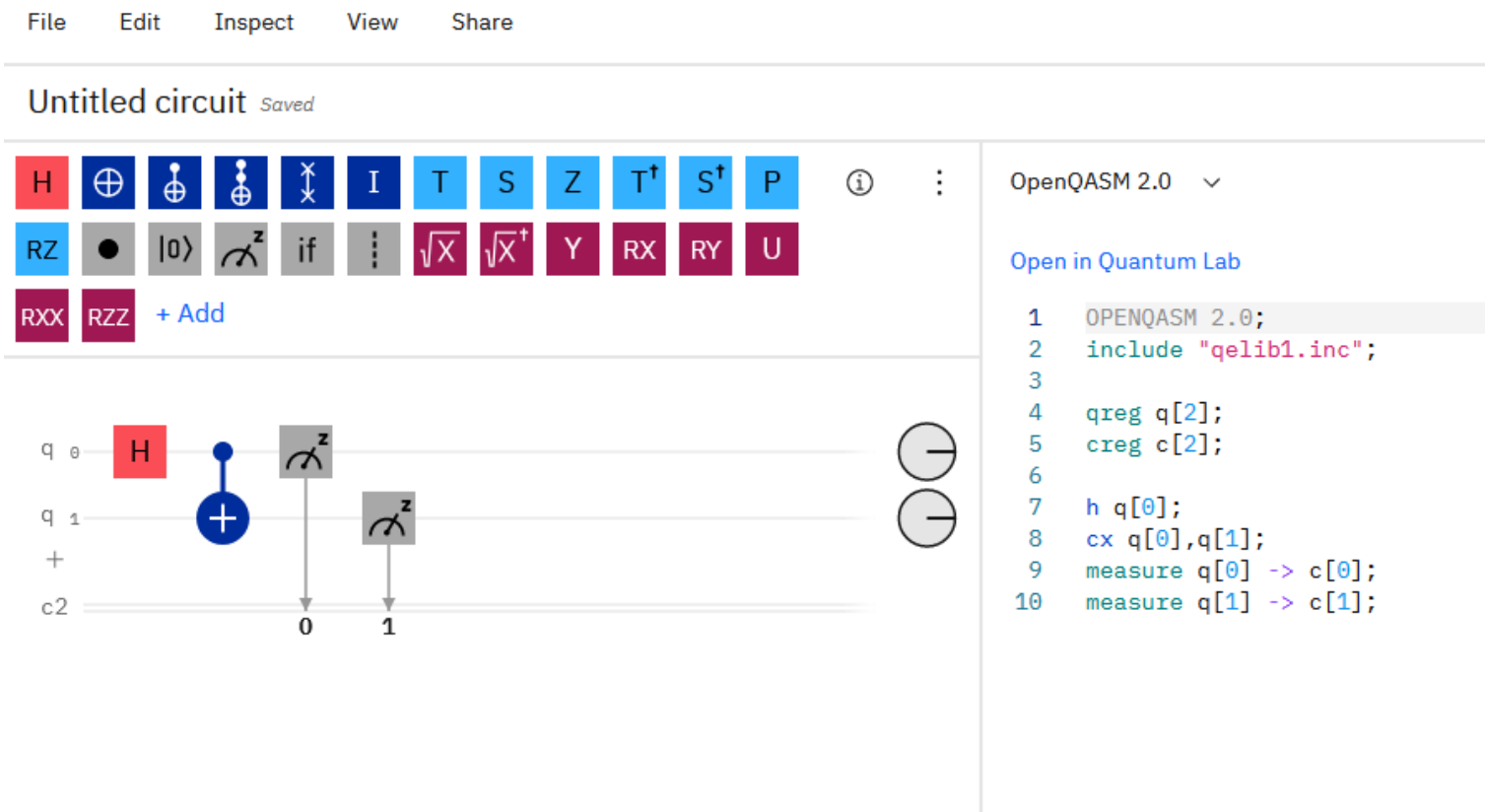
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



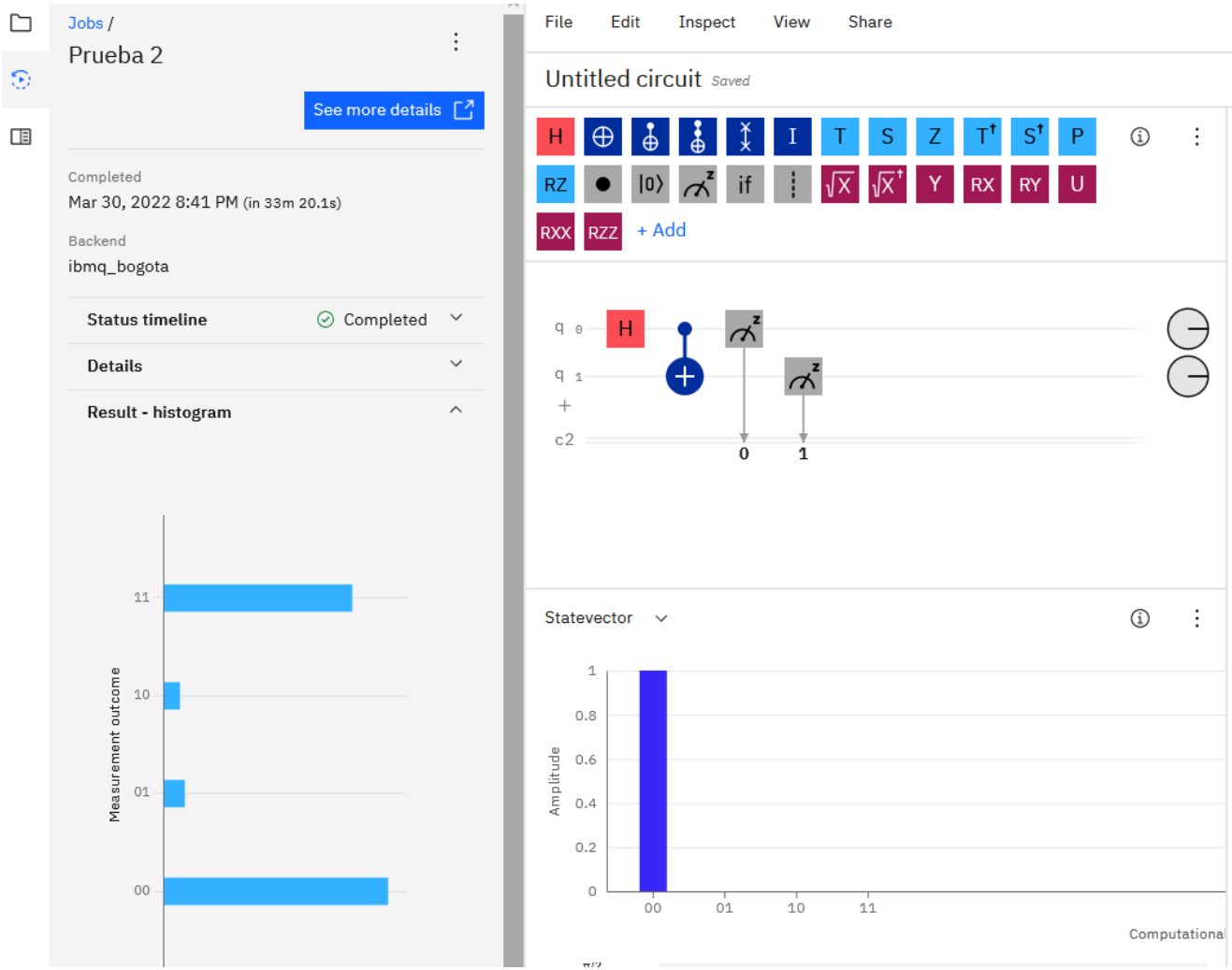
# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



# IBM Quantum Experience

- ✔ Accedemos por medio de Google, buscando IBM Quantum
- ✔ El enlace directo es https://quantum-computing.ibm.com/



Curso de Formación Continua en Computación Cuántica
Curso online organizado por la Escuela Superior de Ingeniería Informática de Albacete
Universidad de Castilla-La Mancha

FIN