COMPUTACIÓN CUÁNTICA

José Joaquín Arias Gómez-Calcerrada

Enero 2017

Modelos de Computación

ÍNDICE

INTRODUCCIÓN

¿Cuánto ocupa un bit?

¿Cuánta información es capaz de almacenar un bit?

¿Qué hay del ruido?

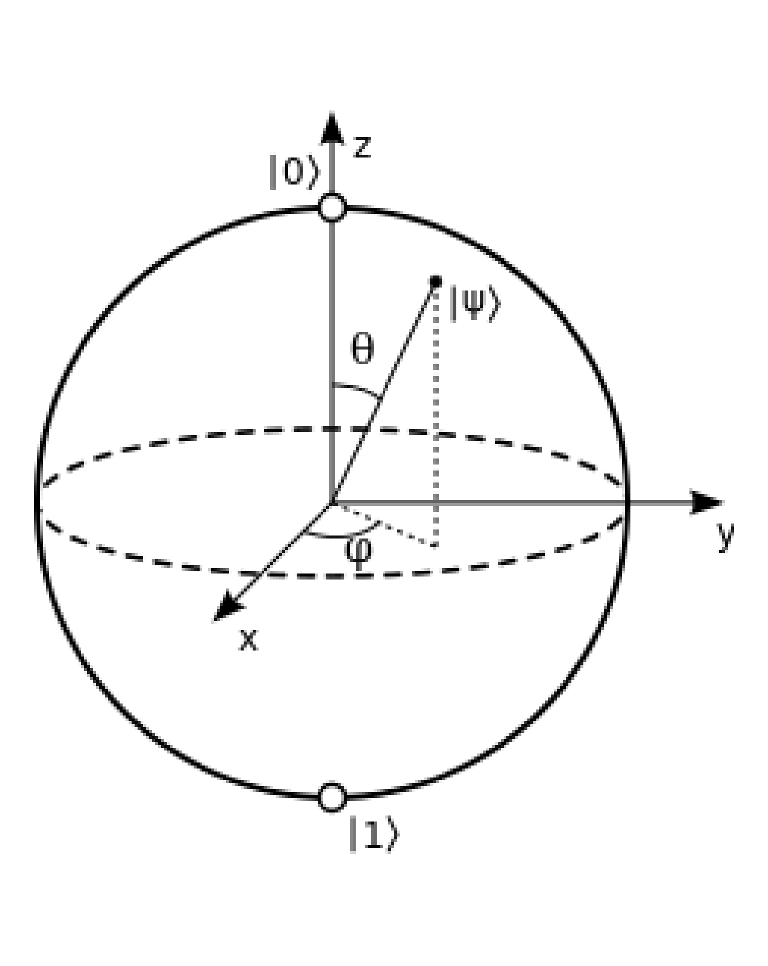
¿Es posible enviar información a través de un canal ruidoso?

DEFINICIÓN DE QUBIT

Se puede entender como un punto en una esfera unitaria del espacio vectorial C^2 .

Un qubit corresponde a la ecuación $x=x_0|0> + x_1|1>$, con $|x_0|^2+|x_1|^2=1$.

El estado -|Ψ> se puede representar como: -|Ψ> = $\cos(\theta/2)|0> + e^{i\phi}\sin(\theta/2)|1>$



TEOREMA DE LA NO CLONACIÓN

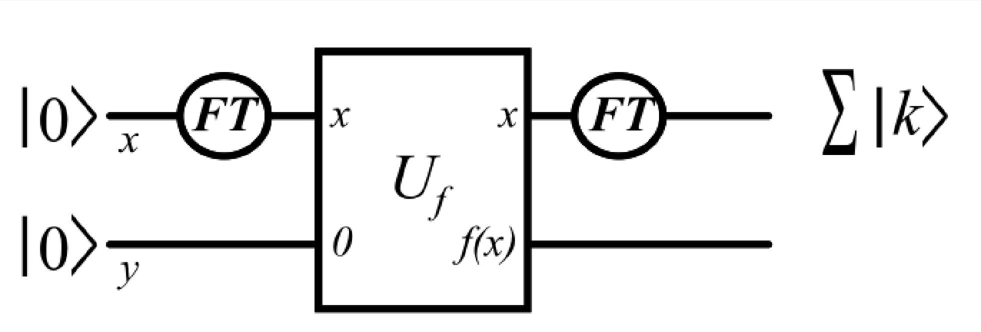
Teorema: Un estado cuántico no conocido no puede ser clonado.

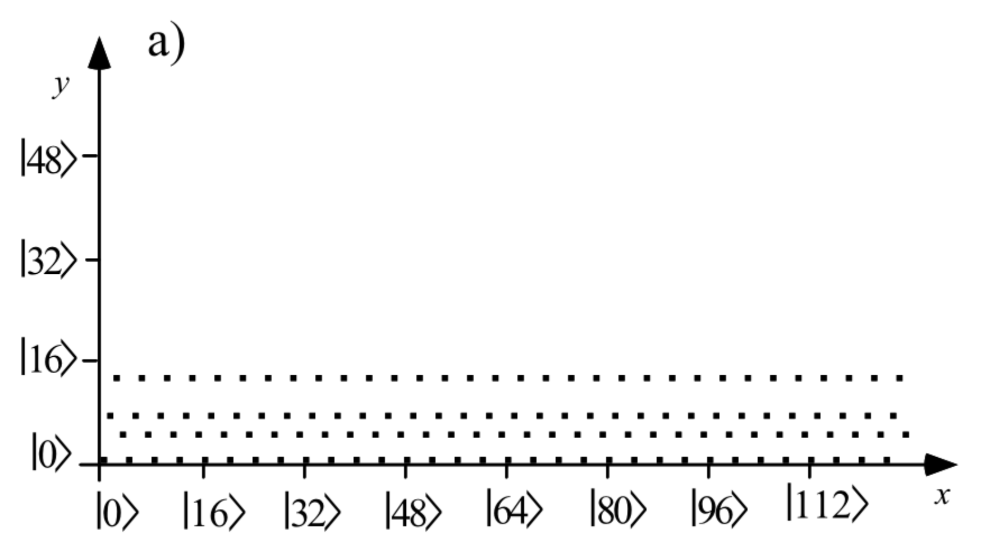
Demostración: Aplicar U de la forma que U(|a> |0>)=|a> |a>. Dado que U no depende de |a>, U(|b> |0>)=|b> |b>. Sin embargo, si tenemos un estado |c> = (|a> + |b>)/√2 , entonces tendremos que U(|c> |0>)=(|a>|a> + |b>|b>)/√2, lo cual no es igual al esperado estado |c> |c>, luego la operación de clonación falla.

Para clonar dos estados estos deben ser ortogonales, es decir, <a|b>=0.

COMPUTADOR CUÁNTICO UNIVERSAL

- Cada qubit debe ser previamente preparado en un estado conocido |0>.
- Cada qubit puede ser medido en la base {|0>, |1>}.
- Una puerta cuántica universal podrá tratar a cualquier conjunto predefinido de qubits.
- Los qubits no pueden evolucionar a estados más allá de sus predeterminados estados.





BÚSQUEDA DEL PERÍODO DE UNA FUNCIÓN Y ALGORITMO DE SHOR

Sea una función f(x) que sea periódica con período r. Asumiendo que a priori no se sabe el período de f(x), lo que podemos hacer en un computador clásico es calcular f(x) para los valores de x y dares cuenta de cuándo se repite dicha función.

En un computador cuántico la cosa cambia.

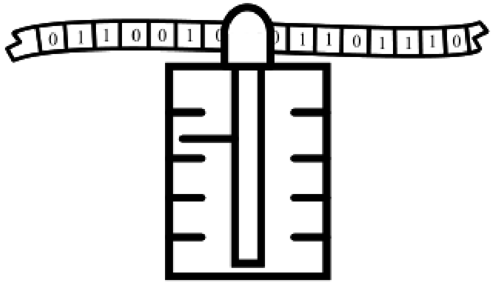
RELACIÓN DE COMPUTACIÓN CUÁNTICA CON MAQUINAS DE TURING: MÁQUINA DE TURING CUÁNTICA

Composición de una máquina de Turing cuántica:

- Una cinta de memoria infinita, solo que cada elemento de ésta es un qubit.
- Un procesador infinito.
- Un cabezal.

$$\mathcal{H} = \left\{ \varphi \mid \varphi : \mathcal{C} \to \mathbb{C}, \sum_{C \in \mathcal{C}} \left|\varphi(C)\right|^2 < \infty \right\}.$$

$$\left| \left|\langle q, T, i | U_{\delta}^{t} | c_0 \rangle\right|^2 - \left|\langle q, T, i | U_{\delta'}^{t+f(t, \frac{1}{\varepsilon})} | c'_0 \rangle\right|^2 \right| < \varepsilon.$$



DEFINICIÓN DE Q-COMPUTABILIDAD

Una función $f : \mathbb{N}^R \to \mathbb{N}$ es computable si existe una máquina de Turing M tal que si $B\xi q_0 1^{[x_1]} 1^{[x_2]} \ldots 1^{[x_k]}$ es la configuración inicial, la configuración final es $\xi p 1^{[y]}$, siendo $y = f(x_1, x_2, \ldots, x_k)$.

$$y = \Phi_M^{(k)}(x_1, x_2, \ldots, x_k)$$

Luego f es parcialmente computable si:

$$f(x_1, x_2, \ldots, x_k) = y = \Phi_M^{(k)}(x_1, x_2, \ldots, x_k)$$

Y f es totalmente computable si:

$$f(x_1, x_2, \ldots, x_k) = y = \Phi_M^{(k)}(x_1, x_2, \ldots, x_k),\ \forall (x_1, x_2, \ldots, x_k) \in \mathbb{N}^k$$

Siendo $\Phi_M^{(k)}(x_1, x_2, \ldots, x_k)$ una computación resultante de aplicar la máquina de Turing M a un conjunto k de qubits, que forman la entrada del programa.