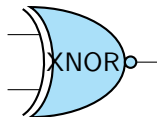
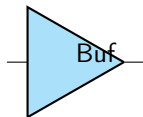
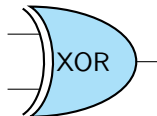
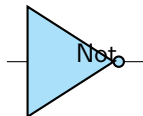
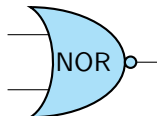
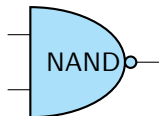
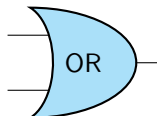
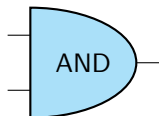
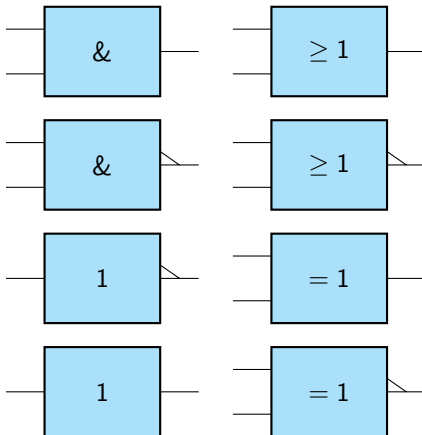


## Porte logiche classiche



## Porte logiche classiche



## Porte logiche quantistiche



I bra e ket sono notazioni sintetiche che si riferiscono a dei vettori. Pertanto  $|0\rangle$  e  $|1\rangle$  possono rappresentare due vettori qualsiasi che formano una base ortonormale in  $\mathbb{C}^2$ .

La base più comunemente utilizzata nel calcolo quantistico è detta *base computazionale*:

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

Un' altra base ortonormale potrebbe essere ad esempio:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \quad |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}$$



# Porte logiche quantistiche



Analogamente a quanto accade nell'informatica classica, le operazioni su un computer quantistico possono essere descritte usando circuiti quantistici costituiti da qubit e porte logiche quantistiche.

Questo concetto é stato introdotto da Deutsch pochi anni dopo l'introduzione del suo algoritmo che definisce l'analogo quantistico di una macchina di Turing.

Nell'informatica classica, ma probabilmente ancora di più nell'informatica quantistica, sebbene i circuiti siano equivalenti dal punto di vista computazionale alle macchine di Turing, di solito sono molto più semplici da rappresentare, manipolare e comprendere.



# Porte logiche quantistiche



Nel calcolo classico, i valori binari del bit passano attraverso le porte logiche per effettuare una semplice operazione. Dato un input binario, la porta logica classica produce un output binario. Le operazioni eseguita dalle porte logiche classiche sono descritte mediante l'algebra booleana.

Le porte logiche quantistiche agiscono allo stesso modo, in quel modo le porte logiche quantistiche applicate mappano lo stato quantistico iniziale ad uno altro stato quantico.

Le porte logiche quantistiche consentono complessivamente di realizzare un processo di evoluzione del sistema da uno stato iniziale ad uno stato finale.



## Porte logiche quantistiche



Le operazioni di calcolo delle porte logiche sono basate sul postulato fondamentale della meccanica quantistica che riguarda l' "Evoluzione dei sistemi quantistici" e che stabilisce quanto segue:

"L'evoluzione di un sistema quantistico chiuso è descritto da una trasformazione unitaria. In altre parole, lo stato  $|\psi\rangle$  del sistema all'istante  $t_1$  è collegato allo stato  $|\psi'\rangle$  del sistema all'istante  $t_2$  da un vettore unitario  $U$  che dipende solo dagli istanti  $t_1$  e  $t_2$ ", cioè:

$$|\psi'\rangle = U|\psi\rangle \quad (1)$$

Il fatto che  $U$  non dipende da  $|\psi\rangle$  ma solo da  $t_1$  e  $t_2$  ha alcune conseguenze dal punto di vista concettuale e computazionale. L'operatore  $U$  è qualcosa che si applica al qubit ma in modo non condizionato dallo stato del qubit stesso. La trasformazione operata dall'operatore avviene indipendentemente dallo stato del qubit.



## Porte logiche quantistiche



Le porte logiche quantistiche sono rappresentate da matrici di trasformazione, o operatori lineari  $U$ .

Gli operatori lineari  $U$  che corrispondono a porte logiche quantistiche devono essere unitari.

Un operatore lineare  $U$  è unitario, se  $U^{-1} = U^\dagger$ , dove  $U^\dagger$  è la trasposta coniugata:  $U^\dagger = \bar{U}^T$ . Ne consegue che  $UU^\dagger = U^\dagger U = I$ .

La composizione di due operatori unitari è ancora un operatore unitario. Date le matrici  $U$  e  $V$  a trasformazione unitaria, si ha:

$$(UV)^\dagger = V^\dagger U^\dagger = V^{-1} U^{-1} = (UV)^{-1} \quad (2)$$



# Porte logiche quantistiche



Esempio 1:

Si consideri il qubit  $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ , si scriva il risultato dell'applicazione a  $|\Psi\rangle$  dell'operatore  $U$ :

$$U = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad (3)$$

Soluzione:

$$|\psi'\rangle = U|\psi\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle \quad (4)$$





## Porte logiche quantistiche



Esempio 2:

Si verifichi che l'operatore  $U$  è unitario:

$$U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (5)$$

Soluzione:

Si deve verificare che  $U^\dagger U = I$ .

$$U^\dagger = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (6)$$

$$U^\dagger U = \frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = I \quad (7)$$



## Porte logiche quantistiche



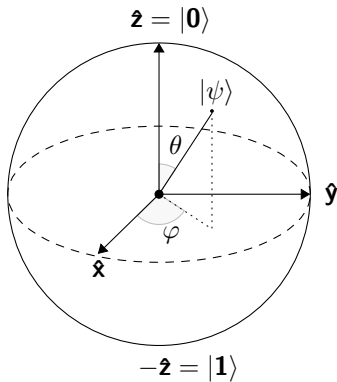
Le trasformazioni unitarie applicate ad un singolo qubit possono essere visualizzate come rotazioni e riflessioni intorno agli assi  $x$ ,  $y$  e  $z$  della sfera di Bloch.

Come si era visto tutte le possibili combinazioni lineari  $\alpha|0\rangle + \beta|1\rangle$  in  $\mathbb{C}^2$  corrispondono ai punti  $(\theta, \psi)$  sulla superficie della sfera unitaria, dove  $\alpha = \cos(\theta/2)$  e  $\beta = e^{i\phi} \sin(\theta/2)$

$$\begin{aligned} |\psi\rangle &= \alpha|0\rangle + \beta|1\rangle \\ &= \cos \frac{\theta}{2} |0\rangle + e^{i\phi} \sin \frac{\theta}{2} |1\rangle \\ &= \cos \frac{\theta}{2} |0\rangle + (\cos \phi + i \sin \phi) \sin \frac{\theta}{2} |1\rangle \end{aligned} \tag{8}$$



# Sfera di Bloch



## Porta logica di Hadamard

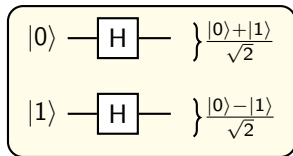


Sebbene in linea di principio qualsiasi trasformazione unitaria  $U$  sia un'operazione valida su un computer quantistico, esiste un numero limitato di operatori che sono considerate porte logiche quantistiche di uso pratico, analogamente alle porte logiche classiche come NOT o XOR, nell'ambito dell'informatica quantistica.

Un importante esempio è l'operatore di Hadamard a singolo-qubit. L'operatore di Hadamard applicato a un qubit con il valore  $|0\rangle$  o  $|1\rangle$  indurrà una sovrapposizione degli stati  $|0\rangle$  e  $|1\rangle$ , con uguale probabilità. L'operatore di Hadamard è anche indicato come "lancio di monete equo",



## Porta logica di Hadamard



$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0| + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1| \quad (9)$$



## Porta logica di Hadamard



Applichiamo quindi l'operatore di Hadamard a  $|0\rangle$

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad (10)$$

e poi a  $|1\rangle$ :

$$H|1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \langle 0|1\rangle + \frac{|0\rangle - |1\rangle}{\sqrt{2}} \langle 1|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (11)$$



## Porta logica di Hadamard



Applichiamo quindi l'operatore di Hadamard al qubit in uscita e otteniamo il qubit in ingresso, come è da aspettarsi essendo l'operatore unitario

$$\begin{aligned} H \left[ \frac{|0\rangle + |1\rangle}{\sqrt{2}} \right] &= \frac{|0\rangle + |1\rangle}{2} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{2} \langle 1|0\rangle + \\ &+ \frac{|0\rangle + |1\rangle}{2} \langle 0|1\rangle + \frac{|0\rangle - |1\rangle}{2} \langle 1|1\rangle \\ &= \frac{|0\rangle + |1\rangle}{2} + \frac{|0\rangle - |1\rangle}{2} \\ &= |0\rangle \end{aligned} \tag{12}$$



## Porta logica di Hadamard



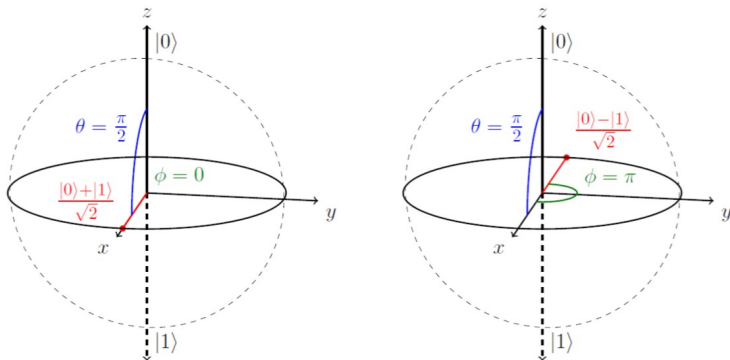
Applichiamo quindi l'operatore di Hadamard all'altro qubit in uscita e otteniamo il qubit in ingresso, come è da aspettarsi essendo l'operatore unitario

$$\begin{aligned} H \left[ \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right] &= \frac{|0\rangle + |1\rangle}{2} \langle 0|0\rangle + \frac{|0\rangle - |1\rangle}{2} \langle 1|0\rangle + \\ &\quad - \frac{|0\rangle + |1\rangle}{2} \langle 0|1\rangle - \frac{|0\rangle - |1\rangle}{2} \langle 1|1\rangle \\ &= \frac{|0\rangle + |1\rangle}{2} - \frac{|0\rangle - |1\rangle}{2} \\ &= |1\rangle \end{aligned} \tag{13}$$





## Porta logica di Hadamard



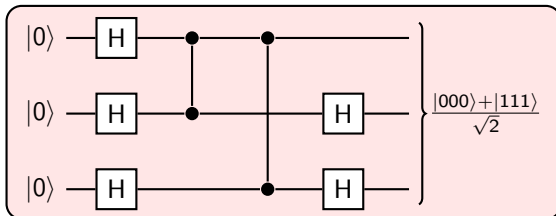
Dal punto di vista geometrico, l'operatore di Hadamard esegue una rotazione di  $\pi/2$  intorno all'asse  $y$  ed una rotazione attorno all'asse  $z$  di  $\pi$  radianti sulla sfera Bloch.



## Porta logica di Hadamard



Molti algoritmi quantistici iniziano applicando l'operatore di Hadamard a ciascun qubit di un registro, il che dà a ciascuna delle possibili configurazioni bit a bit  $2^n$  degli  $n$  qubit una probabilità uguale di  $2^{-n}$  di essere osservata quando il sistema viene misurato.



In questa figura è mostrato un esempio di utilizzo della porta di Hadamard nel circuito quantistico di Greenberger-Horne-Zeilinger (GHZ).

