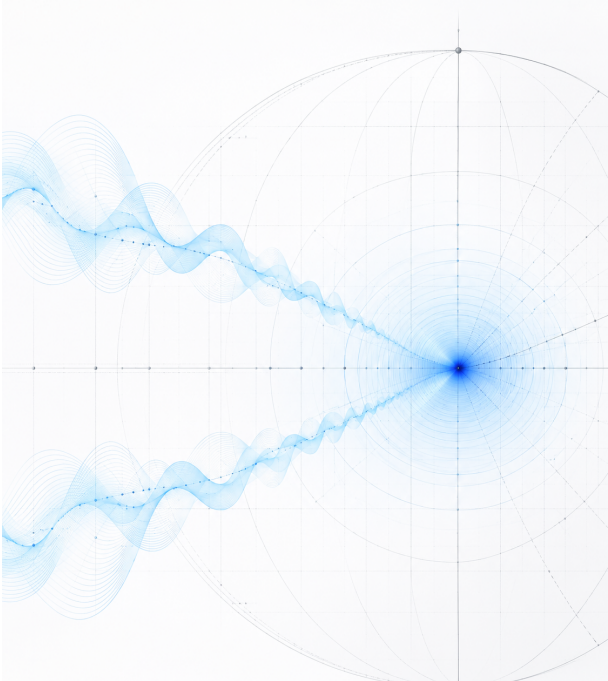
LEZIONE 13–14

Registri, porte e circuiti quantistici

Come si costruiscono e si compongono i circuiti quantistici?

Metodi della Fisica Quantistica per l'Ingegneria

Prof. Vincenzo Berardi · Politecnico di Bari



Registri classici: definizione e configurazioni

Un **registro** è un insieme ordinato di unità elementari di informazione. Nel caso classico contiene n bit, ciascuno con valore 0 oppure 1.

$$x = x_{n-1} \dots x_1 x_0, \qquad x_j \in \{0, 1\}, \qquad \text{configurazioni possibili} = 2^n.$$

Registro	Configurazioni possibili	Esempio
1 bit	2	$0, 1$
2 bit	4	$00, 01, 10, 11$
3 bit	8	$000, 001, 010, 011, 100, 101, 110, 111$

Ogni registro classico ha, in un dato istante, *una configurazione definita*.

Registro quantistico e base computazionale

Un registro di n qubit è descritto nello spazio

$$\mathcal{H}_n = (\mathbb{C}^2)^{\otimes n}, \qquad \dim \mathcal{H}_n = 2^n.$$

Gli stati di base $|x\rangle$ corrispondono alle stringhe classiche x.

Configurazione classica	Stato della base computazionale
00	$\|00\rangle = \|0\rangle \otimes \|0\rangle$
01	$\|01\rangle = \|0\rangle \otimes \|1\rangle$
10	$\|10\rangle = \|1\rangle \otimes \|0\rangle$
11	$\|11\rangle = \|1\rangle \otimes \|1\rangle$

Lo stato generale *non* deve coincidere con uno degli stati di base:

$$|\psi\rangle = \sum_{x=0}^{2^n-1} \alpha_x |x\rangle, \qquad \alpha_x \in \mathbb{C}, \quad \sum_x |\alpha_x|^2 = 1.$$

Misura nella base computazionale: esito, stato e probabilità

Un qubit. Sia $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Una misura nella base computazionale può dare l'*esito classico* 0 oppure 1.

Concetto	Notazione	Significato
Stato associato all'esito 0	$\|0\rangle$	Autostato associato all'esito 0
Esito della misura	0	Valore classico osservato
Stato dopo la misura, se l'esito è 0	$\|0\rangle$	Stato successivo alla misura proiettiva ideale
Probabilità dell'esito 0	$P(0) = \|\alpha\|^2$	Probabilità di osservare 0

Per l'esito 1 valgono analogamente lo stato $|1\rangle$ e la probabilità $P(1) = |\beta|^2$. **Registro di n qubit.**

Misurando tutti i qubit si ottiene una stringa classica di n bit, ognuno uguale a 0 oppure 1. Per $|\Psi\rangle = \sum_{x\in\{0,1\}^n} c_x|x\rangle$, la probabilità della stringa x è $P(x) = |c_x|^2$. Per esempio, l'esito 001 è associato allo stato di base $|001\rangle$.

Esempio: normalizzazione e misura di due qubit

Consideriamo lo stato

$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

La componente $|10\rangle$ ha ampiezza nulla. Verifichiamo la normalizzazione:

$$\langle\psi|\psi\rangle = \left|\frac{1}{2}\right|^2 + \left|\frac{i}{2}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{4} + \frac{1}{4} + \frac{1}{2} = 1.$$

Esito x	00	01	10	11
$p(x) = \lvert\alpha_x\rvert^2$	1/4	1/4	0	1/2

Una misura nella base computazionale restituisce **un solo esito** x, non l'elenco delle ampiezze α_x.

Le fasi relative distinguono stati con le stesse probabilità

Due stati possono dare le stesse statistiche nella base computazionale:

$$|\psi_+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \qquad |\psi_-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}.$$

	$p(00)$	$p(11)$
$\|\psi_+\rangle$	$1/2$	$1/2$
$\|\psi_-\rangle$	$1/2$	$1/2$

Eppure il loro prodotto scalare è

$$\langle\psi_+|\psi_-\rangle = \frac{1}{2}(1-1) = 0.$$

Sono **ortogonali**: il segno relativo (una fase di π) contiene informazione che opportune trasformazioni possono rendere osservabile.

Preparazione di un registro di tre qubit

Inizializzazione. Il registro parte dallo stato noto $|\psi_0\rangle = |000\rangle$. **Preparazione della configurazione $|101\rangle$.** La porta X scambia $|0\rangle$ e $|1\rangle$, mentre I lascia il qubit invariato:

$$|000\rangle \xrightarrow{X\otimes I\otimes I} |100\rangle \xrightarrow{I\otimes I\otimes X} |101\rangle.$$

Preparazione di una sovrapposizione. $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; applicando H al secondo qubit:

$$|101\rangle \xrightarrow{I\otimes H\otimes I} \frac{|101\rangle + |111\rangle}{\sqrt{2}}.$$

Le matrici delle porte X e H saranno studiate nella Sezione 6.3.

Registro classico e quantistico: confronto

Registro classico	Registro quantistico
n bit	n qubit
Una configurazione x alla volta	Stato $\|\psi\rangle$ anche sovrapposto
2^n configurazioni possibili	Spazio di dimensione 2^n
Contenuto rappresentato da bit	Ampiezze complesse α_x
Lettura ideale del contenuto	Probabilità di misura $\|\alpha_x\|^2$
Nessuna fase relativa fra configurazioni	Fasi relative fisicamente significative

Attenzione: 2^n ampiezze non equivalgono a 2^n numeri classici leggibili con una singola misura.

Circuiti classici: composizione e irreversibilità

Un circuito classico realizza una funzione mediante la composizione di operazioni elementari:

$$x \xrightarrow{f} y \xrightarrow{g} z, \qquad z = g(f(x)).$$

La porta AND è un esempio di funzione non invertibile:

a	b	$a \wedge b$
0	0	0
0	1	0
1	0	0
1	1	1

L'uscita 0 ha tre preimmagini: AND non è invertibile.

Circuiti quantistici: composizione e reversibilità

Nella parte unitaria di un circuito quantistico, ogni porta è rappresentata da un operatore unitario:

$$\begin{aligned} |\psi_1\rangle &= U_1|\psi_0\rangle, \\ |\psi_2\rangle &= U_2|\psi_1\rangle = U_2U_1|\psi_0\rangle, \\ |\psi_m\rangle &= U_m \cdots U_2U_1|\psi_0\rangle. \end{aligned}$$

La prima porta applicata si trova a destra nel prodotto. Poiché $U_j^{-1} = U_j^\dagger$,

$$U_{\text{tot}} = U_m \cdots U_1, \qquad U_{\text{tot}}^{-1} = U_1^\dagger \cdots U_m^\dagger.$$

Invertire l'evoluzione ideale significa applicare le porte inverse in ordine opposto.

Ordine delle operazioni e uscita classica

In generale l'ordine delle porte conta: per operatori che non commutano,

$$U_2 U_1 \neq U_1 U_2.$$

L'azione concreta di due operatori, nei due ordini, verrà calcolata dopo aver introdotto le porte elementari. La parte unitaria del circuito prepara lo stato finale

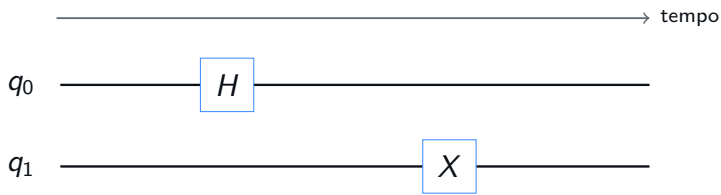
$$|\psi_{\text{out}}\rangle = U_{\text{tot}}|\psi_{\text{in}}\rangle.$$

Se si misura nella base computazionale, la probabilità dell'esito classico x è

$$p(x) = \left|\langle x|\psi_{\text{out}}\rangle\right|^2.$$

Una singola misura restituisce un esito x, non l'intero vettore delle ampiezze.

Un wire identifica un qubit e il tempo scorre da sinistra a destra



VERTICALE

Ogni linea identifica un sottosistema/qubit.

ORIZZONTALE

L'ordine da sinistra a destra codifica la sequenza temporale logica.

Dal circuito astratto al dispositivo quantistico

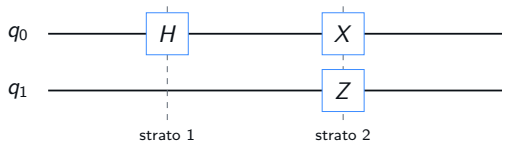
Il programma classico stabilisce la sequenza delle operazioni e riceve gli esiti delle misure; il **registro quantistico** evolve secondo le porte applicate.

Programma e controllo classico: porte, impulsi, lettura degli esiti
$\downarrow$ segnali di controllo
Dispositivo quantistico: qubit fisici, evoluzione, misura
$\downarrow$ esiti di misura
Elaborazione classica dei risultati ed eventuale feedback

Descrizione circuitale astratta	**Implementazione fisica**
Qubit e stato $\lvert\psi\rangle$	Sistema fisico che codifica un qubit
Porta unitaria U	Controlli fisici che realizzano U
Collegamenti nel circuito	Connettività disponibile nel dispositivo
Misura del qubit	Procedura fisica di lettura

Strati circuitali: operazioni successive e in parallelo

Uno **strato circuitale** raccoglie porte applicabili in parallelo su insiemi disgiunti di qubit. Nei diagrammi il tempo procede da sinistra a destra.



$$U_1 = H \otimes I \qquad (H \text{ su } q_0),$$
$$U_2 = X \otimes Z \qquad (X \text{ su } q_0,\ Z \text{ su } q_1),$$
$$U_{\text{tot}} = U_2 U_1 = (X \otimes Z)(H \otimes I).$$

L'allineamento indica parallelismo nel modello circuitale, non necessariamente identici tempi di esecuzione sull'hardware.

La misura collega il wire quantistico a un registro classico



PRIMA DI *M*

Il wire trasporta uno stato quantistico e le porte agiscono unitariamente.

DOPO *M*

L'esito è un bit classico memorizzabile e utilizzabile dal controllo.

Convenzione di ordinamento dei qubit

Nei diagrammi i qubit sono identificati dagli indici $q_0, q_1, \ldots, q_{n-1}$. In questo corso scriveremo gli stati della base computazionale nell'ordine

$$|q_0 q_1 \cdots q_{n-1}\rangle.$$

Per due qubit, la base ordinata e la rappresentazione vettoriale sono:

Stato	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
Vettore	$\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\1\\0\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$	$\begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

La stessa convenzione si applica a prodotti tensoriali, matrici e diagrammi.

Due qubit: espansione del prodotto tensoriale

Siano $|\psi\rangle = a|0\rangle + b|1\rangle$ e $|\phi\rangle = c|0\rangle + d|1\rangle$. Per distributività,

$$\begin{aligned} |\psi\rangle \otimes |\phi\rangle &= (a|0\rangle + b|1\rangle) \otimes (c|0\rangle + d|1\rangle) \\ &= ac|00\rangle + ad|01\rangle + bc|10\rangle + bd|11\rangle. \end{aligned}$$

Nella base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$|\psi\phi\rangle = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

L'ordine dei qubit determina l'ordine delle componenti.

Due qubit: normalizzazione passo per passo

Consideriamo lo stato

$$|\psi\rangle = \frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle.$$

Poiché la base computazionale è ortonormale,

$$\begin{aligned}\langle\psi|\psi\rangle &= \left|\frac{1}{2}\right|^2 + \left|\frac{i}{2}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 \\ &= \frac{1}{4} + \frac{1}{4} + \frac{1}{2} = 1.\end{aligned}$$

Le probabilità degli esiti $00, 01, 10, 11$ sono rispettivamente

$$\left(\frac{1}{4}, \frac{1}{4}, 0, \frac{1}{2}\right).$$

Composizione temporale: perché l'ordine è invertito?

Uno stato iniziale $|\psi_0\rangle$ attraversa dapprima U_1, poi U_2:

$$|\psi_1\rangle = U_1|\psi_0\rangle,$$
$$|\psi_2\rangle = U_2|\psi_1\rangle = U_2U_1|\psi_0\rangle.$$

Per m porte applicate in ordine $U_1, \ldots, U_m$:

$$|\psi_m\rangle = (U_m \cdots U_2U_1)|\psi_0\rangle.$$

L'operatore più vicino al ket agisce per primo.

Composizione: calcolo esplicito di $U_2 U_1$

Poniamo

$$U_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad U_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}, \quad |\psi_0\rangle = |0\rangle.$$

Applicando prima U_1:

$$U_1|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}.$$

Poi U_2:

$$U_2 U_1|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}.$$

Le due probabilità di misura sono $1/2$ e $1/2$.

Invertire l'ordine: calcolo di $U_1 U_2$

Con gli stessi U_1, U_2 e $|\psi_0\rangle = |0\rangle$:

$$U_2|0\rangle = |0\rangle, \qquad U_1 U_2|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

In confronto,

$$U_2 U_1|0\rangle = \frac{|0\rangle + i|1\rangle}{\sqrt{2}}.$$

Le probabilità computazionali sono uguali in questo esempio, ma *gli stati sono differenti*: la fase relativa è diversa.

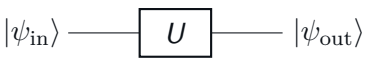
$$U_2 U_1 \neq U_1 U_2.$$

L'ordine delle porte può cambiare lo stato anche quando una singola misura nella base computazionale non lo rivela.

Che cos'è una porta quantistica?

Una **porta quantistica** e un'operazione elementare di elaborazione: per un singolo qubit isolato e rappresentata da una matrice $U \in \mathbb{C}^{2\times 2}$.

$$|\psi_{\text{in}}\rangle \xrightarrow{U} |\psi_{\text{out}}\rangle = U|\psi_{\text{in}}\rangle, \qquad U^\dagger U = I.$$



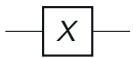
L'unitarieta conserva la normalizzazione:

$$\begin{aligned}\langle\psi_{\text{out}}|\psi_{\text{out}}\rangle &= \langle\psi_{\text{in}}|U^\dagger U|\psi_{\text{in}}\rangle \\ &= \langle\psi_{\text{in}}|\psi_{\text{in}}\rangle = 1.\end{aligned}$$

Attenzione: l'evoluzione unitaria e la misura non sono la stessa operazione.

Porta X: il NOT quantistico

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



$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \quad X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = |0\rangle.$$

Ingresso	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Uscita $X\|\psi\rangle$	$\|1\rangle$	$\|0\rangle$	$\|+\rangle$	$-\|-\rangle$

Porta X: calcolo su una sovrapposizione

La linearita estende l'azione di X dalla base a ogni stato:

$$X(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix}$$
$$= \beta|0\rangle + \alpha|1\rangle.$$

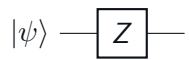
Esempio numerico:

$$X \begin{pmatrix} \sqrt{3}/2 \\ 1/2 \end{pmatrix} = \begin{pmatrix} 1/2 \\ \sqrt{3}/2 \end{pmatrix}.$$

Esito della misura	Prima di X	Dopo X
0	3/4	1/4
1	1/4	3/4

Porta Z: cambiamento della fase relativa

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



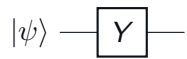
$$Z \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ -\beta \end{pmatrix}.$$

Ingresso	$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$
Uscita $Z\lvert\psi\rangle$	$\lvert 0\rangle$	$-\lvert 1\rangle$	$\lvert -\rangle$	$\lvert +\rangle$

Il segno relativo cambia, mentre $|\alpha|^2$ e $|\beta|^2$ rimangono invariati.

Porta Y: scambio e fattori di fase

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



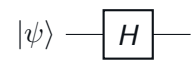
$$Y \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} -i\beta \\ i\alpha \end{pmatrix}.$$

Ingresso	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Uscita $Y\|\psi\rangle$	$i\|1\rangle$	$-i\|0\rangle$	$-i\|-\rangle$	$i\|+\rangle$

I fattori $\pm i$ sono parte del risultato matematico esatto.

Hadamard: tra base computazionale e base X

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



$$H \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}.$$

Ingresso	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Uscita $H\|\psi\rangle$	$\|+\rangle$	$\|-\rangle$	$\|0\rangle$	$\|1\rangle$

Per esempio $H|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle$.

Una fase relativa diventa osservabile dopo Hadamard

Partiamo dallo stato $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.

$$Z|+\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle.$$

Le probabilita computazionali di $|+\rangle$ e $|-\rangle$ sono entrambe $(1/2, 1/2)$; ma dopo H:

$$H|+\rangle = \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |0\rangle,$$

$$HZ|+\rangle = H|-\rangle = \tfrac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |1\rangle.$$

Il primo circuito fornisce sempre 0, il secondo sempre 1 alla misura computazionale.

L'ordine delle porte: esempio con H e X

Le due successioni producono stati diversi a partire da $|0\rangle$:

$$HX|0\rangle = H(X|0\rangle) = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |-\rangle,$$

$$XH|0\rangle = X\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) = \frac{|1\rangle + |0\rangle}{\sqrt{2}} = |+\rangle.$$

Il confronto mostra che $HX \neq XH$. I due stati hanno le stesse probabilità nella base computazionale, ma differiscono per la fase relativa.

Hadamard è auto-inversa: $H^2 = I$

La matrice di Hadamard è

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

Moltiplicando esplicitamente:

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

$$= \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I.$$



Due Hadamard consecutive equivalgono all'identità.

La sequenza HZH realizza la porta X

Le matrici danno esplicitamente

$$HZH = \frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

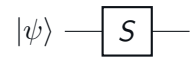
$$= \frac{1}{2}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = X.$$



$$|0\rangle \xrightarrow{H} |+\rangle \xrightarrow{Z} |-\rangle \xrightarrow{H} |1\rangle.$$

Porta S: fase relativa controllata

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



$$S(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + i\beta|1\rangle$$

Ingresso	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Uscita	$\|0\rangle$	$i\|1\rangle$	$(\|0\rangle + i\|1\rangle)/\sqrt{2}$	$(\|0\rangle - i\|1\rangle)/\sqrt{2}$

Porta T: fase relativa controllata

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}$$



$$T(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle + e^{i\pi/4}\beta|1\rangle$$

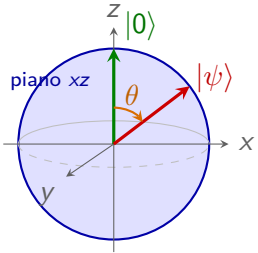
Ingresso	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
Uscita	$\|0\rangle$	$e^{i\pi/4}\|1\rangle$	$(\|0\rangle + e^{i\pi/4}\|1\rangle)/\sqrt{2}$	$(\|0\rangle - e^{i\pi/4}\|1\rangle)/\sqrt{2}$

Significato fisico. Le porte S e T modificano la *fase relativa* tra $|0\rangle$ e $|1\rangle$; l'effetto può essere rivelato con successive operazioni di interferenza. Non introducono semplicemente una fase globale comune.

Rotazioni del qubit: angolo e sfera di Bloch

La trasformazione $R_k(\theta)$ ruota il **vettore di Bloch** di un angolo θ attorno all'asse $k = x, y, z$:

$$R_k(\theta) = \exp\left(-i\frac{\theta}{2}\sigma_k\right), \qquad \sigma_x = X, \quad \sigma_y = Y, \quad \sigma_z = Z.$$



Esempio: $R_y(\theta)$ ruota il vettore iniziale $+z$ verso $+x$ nel **piano** xz. L'angolo geometrico e' θ. *Il fattore* $1/2$ *sara' chiarito nella slide seguente.*

Origine di $\theta/2$: ampiezze e vettore di Bloch

Consideriamo uno stato con ampiezze reali (nel piano xz):

$$|\psi(\alpha)\rangle = \cos\alpha\,|0\rangle + \sin\alpha\,|1\rangle.$$

Le componenti del vettore di Bloch sono $r_k = \langle\psi|\sigma_k|\psi\rangle$. Calcolando:

$$\begin{aligned} r_x &= 2\cos\alpha\sin\alpha = \sin(2\alpha), \\ r_y &= 0, \qquad\qquad \Rightarrow \quad \mathbf{r} = (\sin 2\alpha,\, 0,\, \cos 2\alpha). \\ r_z &= \cos^2\alpha - \sin^2\alpha = \cos(2\alpha). \end{aligned}$$

Il vettore $\mathbf{r}$ forma con $+z$ un angolo 2α. Per una rotazione di θ: $2\alpha = \theta$.

$$\boxed{\alpha = \frac{\theta}{2}} \qquad \Rightarrow \qquad R_y(\theta)|0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle.$$

Rotazioni: sviluppo dell'esponenziale

Per le matrici di Pauli $\sigma_k^2 = I$; pertanto $\sigma_k^3 = \sigma_k$ e $\sigma_k^4 = I$. Sviluppiamo i primi termini della serie esponenziale:

$$\begin{aligned} R_k(\theta) = e^{-i\theta\sigma_k/2} &= I - i\frac{\theta}{2}\sigma_k - \frac{1}{2!}\left(\frac{\theta}{2}\right)^2 I + \frac{i}{3!}\left(\frac{\theta}{2}\right)^3 \sigma_k + \cdots \\ &= I\left[1 - \frac{(\theta/2)^2}{2!} + \frac{(\theta/2)^4}{4!} - \cdots\right] \\ &\quad - i\sigma_k\left[\frac{\theta}{2} - \frac{(\theta/2)^3}{3!} + \frac{(\theta/2)^5}{5!} - \cdots\right]. \end{aligned}$$

Le parentesi sono le serie di Taylor del coseno e del seno:

$$\boxed{R_k(\theta) = I\cos\frac{\theta}{2} - i\sigma_k \sin\frac{\theta}{2}.}$$

Le tre matrici di rotazione: calcolo esplicito

Poniamo $c = \cos(\theta/2)$ e $s = \sin(\theta/2)$. Da $R_k = cI - is\sigma_k$:

$$R_x = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} - is \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} c & -is \\ -is & c \end{pmatrix},$$

$$R_y = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} - is \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} c & -s \\ s & c \end{pmatrix},$$

$$R_z = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} - is \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} c - is & 0 \\ 0 & c + is \end{pmatrix} = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

Per $\theta = \pi$, $R_k(\pi) = -i\sigma_k$: le porte X, Y, Z sono rotazioni di π *a meno di fase globale*.

Rotazione $R_y(\theta)$: stato finale e probabilità

Applicando la matrice a $|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$:

$$R_y(\theta)|0\rangle = \begin{pmatrix} c & -s \\ s & c \end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}c\\s\end{pmatrix} = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle.$$

La misura nella base computazionale fornisce

$$P(0) = \cos^2\frac{\theta}{2}, \qquad P(1) = \sin^2\frac{\theta}{2}.$$

θ	Stato $R_y(\theta)\|0\rangle$	$P(0)$	$P(1)$
0	$\|0\rangle$	1	0
$\pi/3$	$\frac{\sqrt{3}}{2}\|0\rangle + \frac{1}{2}\|1\rangle$	$3/4$	$1/4$
$\pi/2$	$\|+\rangle$	$1/2$	$1/2$
π	$\|1\rangle$	0	1

Inversi e composizioni

Porte inverse

Porta	Inversa
X, Y, Z, H	La porta stessa
S	$S^\dagger$
T	$T^\dagger$

Composizioni delle porte di fase

Composizione	Risultato
T^2	S
S^2	Z
T^4	Z
S^4	I

Verifica mediante prodotto matriciale:

$$T^2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/2} \end{pmatrix} = S.$$

Prevedere qualitativamente prima di moltiplicare le matrici

DOMANDA 1

La porta cambia i moduli delle ampiezze o soltanto le fasi?

DOMANDA 2

La porta è auto-inversa? Quale base rende semplice la sua azione?

Una previsione qualitativa riduce errori e rende il calcolo matriciale un controllo, non un procedimento cieco.

Hadamard su uno stato generale

Scriviamo $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, ossia

$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}.$$

Dalla matrice di Hadamard segue

$$\begin{aligned} H|\psi\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \\ &= \frac{1}{\sqrt{2}} \begin{pmatrix} \alpha + \beta \\ \alpha - \beta \end{pmatrix}. \end{aligned}$$

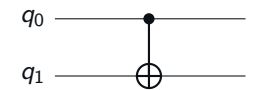
Quindi

$$H|\psi\rangle = \frac{\alpha + \beta}{\sqrt{2}}|0\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle.$$

CNOT: controllo, bersaglio e somma modulo 2

La CNOT agisce su due qubit: q_0 (**controllo**) e q_1 (**bersaglio**). Negli stati della base computazionale il controllo non cambia; il bersaglio viene invertito se il controllo vale 1.

c	t	c_{out}	$t_{\text{out}} = t \oplus c$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



$$\mathrm{CNOT}|c, t\rangle = |c, t \oplus c\rangle.$$

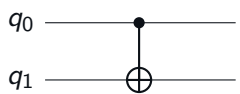
La **somma modulo 2** ($\oplus$) determina l'etichetta binaria del bersaglio: $0 \oplus 0 = 0$, $0 \oplus 1 = 1$, $1 \oplus 0 = 1$, $1 \oplus 1 = 0$.

Attenzione: c e t identificano gli stati della base, *non* esiti di misure eseguite durante la porta.

CNOT: matrice e azione su uno stato generale

Nella base ordinata $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$



Per uno stato arbitrario $|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$:

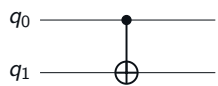
$$\mathrm{CNOT} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}, \qquad \mathrm{CNOT}|\psi\rangle = a|00\rangle + b|01\rangle + d|10\rangle + c|11\rangle.$$

La porta scambia le ampiezze di $|10\rangle$ e $|11\rangle$ **senza misurare** il controllo.

CNOT: una sovrapposizione può diventare entangled

Partiamo da due qubit in uno **stato separabile**, con il controllo in sovrapposizione:

$$|\psi_{\text{in}}\rangle = |+\rangle|0\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$



La CNOT agisce linearmente sui due termini, senza misurare il controllo:

$$\begin{aligned}\text{CNOT}|\psi_{\text{in}}\rangle &= \frac{\text{CNOT}|00\rangle + \text{CNOT}|10\rangle}{\sqrt{2}} \\ &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle.\end{aligned}$$

Lo stato $|\Phi^+\rangle$ non si fattorizza in stati dei singoli qubit: **è entangled**.
Controesempio: $\text{CNOT}|00\rangle = |00\rangle$ rimane separabile.

Una controlled-U generalizza il meccanismo controllo–bersaglio

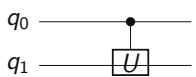
CONTROLLO 0

$$|0\rangle|\psi\rangle \mapsto |0\rangle|\psi\rangle$$

CONTROLLO 1

$$|1\rangle|\psi\rangle \mapsto |1\rangle U|\psi\rangle$$

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$



Controlled-Z (CZ): fase sullo stato $|11\rangle$

La porta CZ lascia invariati $|00\rangle$, $|01\rangle$ e $|10\rangle$, ma cambia il segno di $|11\rangle$.

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

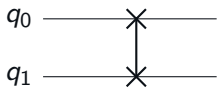


Ingresso	Uscita
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|10\rangle$
$\|11\rangle$	$-\|11\rangle$

SWAP: scambio dei due qubit

La porta SWAP scambia gli stati dei due qubit: $\mathrm{SWAP}|a, b\rangle = |b, a\rangle$.

$$\mathrm{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$



Ingresso	Uscita
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|10\rangle$
$\|10\rangle$	$\|01\rangle$
$\|11\rangle$	$\|11\rangle$

Porta Toffoli (CCNOT): funzionamento e AND reversibile

La **Toffoli** agisce su tre qubit: due controlli a, b e un bersaglio c. Il bersaglio cambia soltanto quando $a = b = 1$:

$$|a, b, c\rangle \longmapsto |a, b, c \oplus ab\rangle.$$

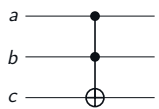


Diagramma CCNOT

Ingresso	Uscita	Ingresso	Uscita
$\|000\rangle$	$\|000\rangle$	$\|100\rangle$	$\|100\rangle$
$\|001\rangle$	$\|001\rangle$	$\|101\rangle$	$\|101\rangle$
$\|010\rangle$	$\|010\rangle$	$\|110\rangle$	$\|111\rangle$
$\|011\rangle$	$\|011\rangle$	$\|111\rangle$	$\|110\rangle$

Tabella di verità nella base computazionale

Applicazione: AND reversibile. Preparando il terzo qubit nello stato $|0\rangle$ si ottiene

$$\boxed{|a, b, 0\rangle \xrightarrow{\text{Toffoli}} |a, b, ab\rangle}.$$

Il terzo qubit contiene $a \wedge b$, mentre i due ingressi restano disponibili: **la trasformazione complessiva rimane reversibile**.

Circuito composto: primo strato $H \otimes X$

Stato iniziale: $|\psi_0\rangle = |00\rangle = |0\rangle \otimes |0\rangle$.



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

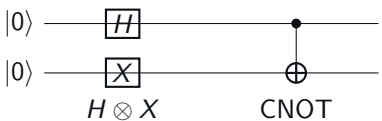
$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi_1\rangle = (H \otimes X)|00\rangle = (H|0\rangle) \otimes (X|0\rangle)$$

$$= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |1\rangle = \boxed{\frac{|01\rangle + |11\rangle}{\sqrt{2}}}.$$

Circuito composto: CNOT e stato finale

Ripartiamo dal risultato del primo strato: $|\psi_1\rangle = (|01\rangle + |11\rangle)/\sqrt{2}$.



Nella base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$|\psi_2\rangle = \mathrm{CNOT}|\psi_1\rangle$$
$$= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \boxed{\frac{|01\rangle + |10\rangle}{\sqrt{2}}}.$$

$$\boxed{U_{\mathrm{tot}} = \mathrm{CNOT}(H \otimes X)}, \qquad |\psi_2\rangle = U_{\mathrm{tot}}|00\rangle.$$

CNOT: calcolo matriciale completo

Nella base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, poniamo

$$M = \mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

L'azione sullo stato generico si ottiene moltiplicando righe per colonne:

$$M \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}.$$

Le componenti associate a $|10\rangle$ e $|11\rangle$ vengono scambiate.

Preparazione di Bell: azione sui due termini

Partiamo dallo stato prodotto $|00\rangle$. Applichiamo H al primo qubit:

$$(H \otimes I)|00\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Applichiamo CNOT con controllo sul primo qubit:

$$\begin{aligned} \mathrm{CNOT}\frac{|00\rangle + |10\rangle}{\sqrt{2}} &= \frac{\mathrm{CNOT}|00\rangle + \mathrm{CNOT}|10\rangle}{\sqrt{2}} \\ &= \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle. \end{aligned}$$

L'unitaria su due qubit può trasformare uno stato prodotto in uno entangled.

Controlled-U: controllo in sovrapposizione

La porta controllata è

$$C(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U.$$

Per un ingresso $(\alpha|0\rangle + \beta|1\rangle) \otimes |\phi\rangle$:

$$\begin{aligned} C(U)(\alpha|0\rangle + \beta|1\rangle)|\phi\rangle &= \alpha|0\rangle I|\phi\rangle + \beta|1\rangle U|\phi\rangle \\ &= \alpha|0\rangle|\phi\rangle + \beta|1\rangle U|\phi\rangle. \end{aligned}$$

L'azione è coerente su entrambi i rami del controllo.

Controlled-Z e CNOT: relazione per coniugazione

Sappiamo che $HXH = Z$ e dunque $HZH = X$. La controlled-Z è

$$CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z.$$

Inserendo H prima e dopo sul bersaglio:

$$\begin{aligned}(I \otimes H)CZ(I \otimes H) &= |0\rangle\langle 0| \otimes (HIH) \\ &\quad + |1\rangle\langle 1| \otimes (HZH) \\ &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \\ &= \mathrm{CNOT}.\end{aligned}$$