

RIPASSONE  
X ESAME

QUANTUM  
COMPUTING

Dianne Cipolla /

# QUBIT

**Cos'è?** Un bit quantistico (qubit) è l'unità di informazione utilizzata per codificare i dati nel quantum computing e può essere inteso come l'equivalente quantistico del bit tradizionale.

**Qubit vs Bit** Un bit classico può esistere solo in posizioni 0 o 1. I qubit possono occupare anche un terzo stato noto come **sovrapposizione**. Una sovrapposizione rappresenta 0, 1 e tutte le posizioni intermedie contemporaneamente (per un totale di 3 posizioni).

Per rappresentare questa tipologia di stati abbiamo bisogno che un qubit venga rappresentato da 2 bit classici con una possibilità di combinazione pari a  $2^2 = 4$  possibili rappresentazioni:

- 1. 00 → stato 0
- 2. 01 → sovrapposizione
- 3. 10 → sovrapposizione
- 4. 11 → stato 1

## Rappresentarli - Notazione di Dirac

**|a> [vetto di a]**: vettore colonna che ha 1 nel punto in cui corrisponde a e 0 per tutti gli altri elementi.

ESEMPIO:  $|0> = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ ;  $|1> = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

**<a| [bra di a]**: vettore riga che funziona come vet.

ESEMPIO:  $\langle 0| = (1 \ 0)$ ;  $\langle 1| = (0 \ 1)$

Ora se doveremo moltiplicare il vettore **|a|** per il vettore **|b>** due cose accadono:

$$\langle a|b> = \begin{cases} 1 & a=b \\ 0 & a \neq b \end{cases} = [\text{braket di } a \text{ e } b]$$

Quindi nel caso in cui moltiplichiamo un vettore riga per uno colonna ottieniamo uno scalare:

$$\begin{pmatrix} * \\ * \\ \vdots \\ * \\ * \end{pmatrix} \begin{pmatrix} * & * & * \\ * & * & * \\ \vdots & \vdots & \vdots \\ * & * & * \\ * & * & * \end{pmatrix} = (* \cdot * + * \cdot * + \dots + * \cdot *) = *$$

Nel caso in cui moltiplichiamo un vettore colonna per un vettore riga ottieniamo una matrice di  $\dim(a \times b)$ :

$$\begin{pmatrix} * \\ * \\ \vdots \\ * \\ * \end{pmatrix} \begin{pmatrix} * & * & * \\ * & * & * \\ \vdots & \vdots & \vdots \\ * & * & * \\ * & * & * \end{pmatrix} = \begin{pmatrix} * & * & * \\ * & * & * \\ \vdots & \vdots & \vdots \\ * & * & * \\ * & * & * \end{pmatrix}$$

## Stato probabilistico

Matematicamente lo stato di un qubit è rappresentato da una combinazione lineare (sovrapposizione) di due stati base  $|0>$  e  $|1>$ :

$$|ψ> = \alpha|0> + \beta|1>$$

dove  $\alpha$  e  $\beta$  sono ampiezze di probabilità, che sono numeri complessi.

Finché il qubit non viene misurato, esso esiste in una sovrapposizione di stati, tuttavia, quando effeguiamo una misurazione, il qubit collassa in modo probabilistico in uno dei due stati:

- Con probabilità  $|\alpha|^2$  il qubit si troverà nello stato  $|0>$
- Con probabilità  $|\beta|^2$  il qubit si troverà nello stato  $|1>$

Dopo la misurazione il qubit non è più in sovrapposizione, ma assume un valore classico definitivo.

**[ATTENZIONE!]** La condizione di normalizzazione impone che  $|\alpha|^2 + |\beta|^2 = 1$ .

ESEMPIO:  $|ψ> = \frac{1}{\sqrt{2}}|0> + \frac{1}{\sqrt{2}}|1>$ . Calcoliamo la probabilità che esca 0 o 1.

$$P_0(0) = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2} \quad P_1(1) = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$1 = P_0(0) + P_1(1) \rightarrow 1 = \frac{1}{2} + \frac{1}{2} \rightarrow 1 = \frac{2}{2} \rightarrow 1 = 1 \quad \checkmark$$

**Entanglement quantistico** Quando 2 qubit sono entangled, entrambi esistono in una sovrapposizione finché uno dei due non viene misurato. Una volta osservato uno di essi, la sovrapposizione quantistica di entrambi i qubit viene compresa e il qubit non osservato assume la posizione opposta rispetto a quello osservato.

ESEMPIO: Rappresentiamo uno stato quantistico di due qubit in sovrapposizione:  $\frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$

Per dimostrare che questo stato è entangled, basta dimostrare che esso non è un stato del prodotto.

Se fosse uno stato prodotto esisterebbero i due vettori quantistici per cui:

$$|0> \otimes |0> = \frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$$

Questo causerebbe la necessità di avere gli stati intermedi ( $|01>$  e  $|10>$ ) con probabilità pari a zero:

$$|0> = a|0> + b|1> \quad |1> = c|0> + d|1> \Rightarrow |0> \otimes |1> = (a|0> + b|1>) \otimes (c|0> + d|1>) = ac|00> + ad|01> + bc|10> + bd|11>$$

probabilità:

$$ac = \frac{1}{\sqrt{2}}; ad = 0; bc = 0; bd = \frac{1}{\sqrt{2}}$$

Ma imponendo queste restrizioni per avere  $ad = bc = 0$  dovremmo avere  $(a + d) = 0 \wedge (b + c) = 0$ , in tal caso non potremmo mai avere la probabilità di  $ac = bd = \frac{1}{\sqrt{2}}$ .

→ Dunque lo stato  $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$  NON può essere scritto come prodotto tensoriale, di conseguenza si tratta di uno stato entangled.

Gli stati più conosciuti entangled sono gli **stati di Bell**:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

Proprietà:

- Sono **entangled**; → qualiasi stato di un sistema a due qubit può essere espresso come combinazione lineare degli stati di Bell.
- Formano una **basis ortonormale** → vedrai prossimamente;
- Sono **invarianti** rispetto alle **trasformazioni globali** → se si applica la stessa operazione unitaria (vedi dopo) su entrambi i qubit, la struttura dello stato rimane invariata;
- Utilizzati nel **teletrasporto quantistico** e nella **codifica quantistica**;

**Operazioni Unitarie** le operazioni sui vettori di stato quantistico sono rappresentate da matrici unitarie.

Una matrice quadrata  $U$  è unitaria se soddisfa la seguente uguaglianza:  $U^\dagger U = I = U U^\dagger$  ( $I$  = mat. identità).

Esse vengono utilizzate in QC poiché preservano la norma dei vettori, il che significa che non alterano la probabilità totale di uno stato quantistico.

ESEMPI DI MATERICI UNITARIE

1. Operazioni Pauli (sono Hermitiane e Unitarie)

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

anche chiamate flip bit

2. Operazione Hadamard

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

Un operatore  $A$  è **Hermitiano** se  $A^\dagger = A$

3. Operazione Phase

$$P_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

**Insiemi ortogonali e ortonomali** Due vettori  $|1\rangle$  e  $|0\rangle$  si dicono **ortogonali** se il solo prodotto interno è zero:  $\langle 1|0\rangle = 0$ . Un insieme di vettori  $\{|1_1\rangle, |1_2\rangle, \dots, |1_m\rangle\}$  è chiamato **insieme ortogonale** se ogni vettore dell'insieme è ortogonale ad ogni altro vettore dell'insieme: se  $\langle 1_j|1_k\rangle = 0$ , per tutte le scelte di  $j, k \in \{1, \dots, m\}$ .

Un insieme di vettori  $\{|1_1\rangle, |1_2\rangle, \dots, |1_m\rangle\}$  è chiamato **insieme ortonormale** se è un insieme ortogonale e, inoltre, ogni vettore nell'insieme è un vettore **unitario** (con modulo = 1). In altre parole, questo insieme è un insieme ortonormale se abbiano:

$$\langle 1_j|1_k\rangle = \begin{cases} 1 & j=k \\ 0 & j \neq k \end{cases} \quad \text{per tutte le scelte di } j, k \in \{1, \dots, m\}$$

[ATTENZIONE!] Algebra: modulo di un vettore

$v$  è un vettore unitario se soddisfa:

$\|v\|=1$ , dove  $\|v\|$  è la norma/modulo del vettore, che viene calcolata come:

$$\|v\| = \sqrt{x_1^2 + x_2^2 + \dots + x_n^2} \quad \text{per un vettore}$$

$$v = (x_1, x_2, \dots, x_n) \in \mathbb{R}^n$$

Come ottengo un vettore unitario?

Supponiamo che  $v$  non sia unitario, per farlo diventare dovrà seguire le seguenti formule:  $u = \frac{v}{\|v\|}$

## [ATTENZIONE!] Algebra: Ripasso AUTOVALORI e AUTOVETTORI

(laura)

Sia  $A$  una matrice quadrata di dimensione  $n \times n$ . Un numero  $\lambda$  è detto **AUTOVALORE** di  $A$  se esiste un vettore non nullo  $\mathbf{v}$  tale che:  $A\mathbf{v} = \lambda\mathbf{v}$ , dove  $\mathbf{v}$  è detto **AUTOVETTORE** associato ad  $\lambda$ .

Come si trovano gli autovalori?

Per trovare gli autovalori di una matrice  $A$ , bisogna risolvere l'equazione caratteristica:

$\det(A - \lambda I) = 0$ , dove  $I$  è la mat. Identità che viene moltiplicata per  $\lambda$ .  $\det(\dots)$  è il determinante della matrice al suo interno.

Come si trovano gli autovettori?

Per ogni valore  $\lambda$ , gli autovettori si trovano risolvendo il sistema lineare:  $(A - \lambda I)\mathbf{v} = 0$ .

Vediamo un **ESEMPIO** pratico:

Sia la matrice  $A = \begin{bmatrix} 4 & -2 \\ 1 & 1 \end{bmatrix}$

Troviamo gli **autovalori**:  $\det(A - \lambda I) = 0$

$$\det \left[ \begin{pmatrix} 4 & -2 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} \right] = 0 \rightarrow \det \left[ \begin{pmatrix} 4-\lambda & -2 \\ 1 & 1-\lambda \end{pmatrix} \right] = 0 \rightarrow \det \left[ \begin{pmatrix} 4-\lambda & -2 \\ 1 & 1-\lambda \end{pmatrix} \right] = 0$$

calcoliamo il determinante

$$\det \left[ \begin{pmatrix} 4-\lambda & -2 \\ 1 & 1-\lambda \end{pmatrix} \right] = 0 \rightarrow [(4-\lambda)(1-\lambda)] - [(-2)(1)] = 0 \rightarrow (4-\lambda)(1-\lambda) + 2 = 0 \rightarrow 6 - 5\lambda + \lambda^2 = 0 \rightarrow (\lambda-2)(\lambda-3) = 0$$

Troviamo gli **autovettori**: Per ogni autovalore, risolviamo  $(A - \lambda I)\mathbf{v} = 0$

Autovettore per  $\lambda_1 = 2$

$$(A - 2I) = \left[ \begin{pmatrix} 4 & -2 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right] = \left[ \begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix} \right]$$

$$\begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \rightarrow \begin{cases} 2x - 2y = 0 \\ x - y = 0 \end{cases} \rightarrow \begin{cases} x = y \\ x = y \end{cases} \rightarrow \text{Quindi abbiamo che un possibile autovettore è} \\ \hookrightarrow \text{applichiamo il vettore } \mathbf{v} \text{ e risolviamo il sistema} \quad \mathbf{v} = \begin{bmatrix} 1 \\ 1 \end{bmatrix} \text{ (in questo caso } x = y)$$

Autovettore per  $\lambda_2 = 3$

$$(A - 3I) = \left[ \begin{pmatrix} 4 & -2 \\ 1 & 1 \end{pmatrix} - \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix} \right] = \left[ \begin{pmatrix} 1 & -2 \\ 1 & -2 \end{pmatrix} \right]$$

$$\begin{pmatrix} 1 & -2 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = 0 \rightarrow \begin{cases} x - 2y = 0 \\ x - 2y = 0 \end{cases} \rightarrow \begin{cases} x = 2y \\ 2y - 2y = 0 \end{cases} \rightarrow \begin{cases} x = 2y \\ 0 = 0 \end{cases} \rightarrow \text{Quindi abbiamo che i possibili autovettori in} \\ \text{questo caso sono:}$$

$$\mathbf{v} = \begin{bmatrix} 2 \\ 1 \end{bmatrix} \text{ oppure } \mathbf{v} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \text{ ecc.}$$

Associamo ciò che abbiamo imparato ai Qubit

Un qubit viene descritto genericamente come:  $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ , dove  $|0\rangle$  e  $|1\rangle$  sono gli **AUTOVETTORI**. Gli operatori sono rappresentati da matrici Hermitiane che agiscono sui qubit. Gli **AUTOVALORI** di questi operatori rappresentano i risultati possibili delle misurazioni.

ESEMPIO: Operatore di Pauli

(Se un operatore è già scritto in forma diagonale, allora i suoi autovalori si trovano direttamente su di esso)

$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$  i suoi autovalori sono  $1$  e  $-1$  e i corrispondenti autovettori sono proprio gli stati base  $|0\rangle$  e  $|1\rangle$ :  $\sigma_z|0\rangle = |1\rangle$   $\sigma_z|1\rangle = -|1\rangle$

$(A|q\rangle = \lambda|q\rangle \rightarrow \text{autovettore} \rightarrow \text{autovalore})$

## Osservabili e operatori Hermitiani

In meccanica quantistica, ogni **osservabile** (una grandezza fisica che può essere misurata) è rappresentata da un **operatore Hermitiano** che agisce su uno spazio di Hilbert. L'operatore Hermitiano rappresenta l'osservabile in modo tale che le sue proprietà matematiche siano in accordo con quelle fisiche.

Lo **spectrum** di un operatore è l'insieme di tutti i suoi autovalori. Questi rappresentano i possibili risultati delle misurazioni dell'osservabile associato.

Ad esempio: immaginiamo di misurare l'energia di una particella in un sistema quantistico, l'operatore a questo osservabile è  $H$  (operatore Hamiltoniano). Gli autovalori di  $H$  rappresentano le possibili energie che possiamo misurare nel sistema.

Dopo una misurazione dell'osservabile  $A$  con autovalori  $a_n$ , il sistema **collassa** in uno stato corrispondente all'autovettore associato all'autovalore  $a_n$ .

**ESEMPIO:** consideriamo un qubit nello stato  $|+\rangle = \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|-\rangle$  dove  $|1\rangle$  e  $|-\rangle$  sono gli autostati dell'operatore di Pauli  $\sigma_2$  con autovalori rispettivamente  $+1$  e  $-1$ .

Se misuriamo quel qubit, possiamo ottenere come risultati  $+1$  o  $-1$ , nel caso in cui otteniamo  $+1$  allora lo stato collassa in  $|1\rangle$ , al contrario, se otteniamo  $-1$  lo stato collasserebbe in  $|-\rangle$ .

Dopo la misura, lo stato  $|+\rangle$  non c'è più una sovrapposizione, ma è stato proiettato su uno degli stati propri dell'operatore misurato.

## Interpretazione geometrica

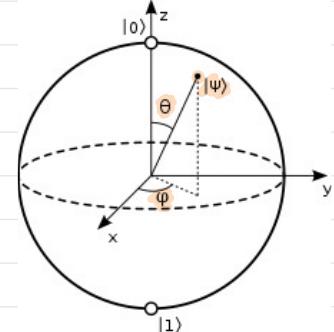
Una visualizzazione utile di un qubit si può ottenere mediante un'interpretazione geometrica che associa gli stati di un qubit ai punti sulla superficie di una sfera di raggio unitario. Il polo sud corrisponde a  $1$  e quello nord a  $0$ . Le altre locazioni sono le sovrapposizioni quantistiche di  $0$  e di  $1$ .

Questa sfera è nota come **sfera di Bloch** rappresentata nell'immagine →

Esiste una corrispondenza biunivoca tra un generico stato di un qubit

$|+\rangle = \alpha|0\rangle + \beta|1\rangle$  e un punto sulla sfera unitaria in  $\mathbb{R}^3$  rappresentato come

$|(\theta, \varphi)\rangle = \cos(\frac{\theta}{2})|0\rangle + e^{i\varphi} \sin(\frac{\theta}{2})|1\rangle$ , dove  $\theta$  e  $\varphi$  sono numeri reali (le coordinate sferiche nel punto).



Quando si applica un operatore unitario  $U$  a un qubit, esso trasforma lo stato quantistico senza alterare la norma. Geometricamente, questo corrisponde a una **rotazione della sfera di Bloch**.

Ad esempio l'operatore di Pauli  $\sigma_x$  ruota il vettore attorno all'asse delle  $x$  di  $180^\circ$  (in effetti scambia  $|0\rangle$  con  $|1\rangle$ ).

Per lo stesso motivo, dunque, gli operatori  $\sigma_z$  e  $\sigma_y$  ruotano rispettivamente intorno all'asse  $z$  e  $y$ .

L'**operatore di rotazione** generale è dato dalla seguente formula:  $R_\sigma(\theta) = e^{-i\frac{\theta}{2}\sigma}$  dove:

-  $\theta$  è l'angolo di rotazione

-  $\sigma = (x, y, z)$  sono le matrici di Pauli

Se un operatore  $A$  verifica l'uguaglianza  $A^2 = \mathbb{I}$  (mat. identità), allora:  
 $e^{-i\frac{\theta}{2}A} = \cos(\frac{\theta}{2})\mathbb{I} - i\sin(\frac{\theta}{2})A$

Visto che le matrici di Pauli verificano  $x^2 = y^2 = z^2 = \mathbb{I}$ , possiamo scrivere le rotazioni intorno agli assi come segue:

- Rotazione intorno all'asse delle  $x$ :

$$R_x(\theta) = e^{-i\frac{\theta}{2}x} = \cos(\frac{\theta}{2})\mathbb{I} - i\sin(\frac{\theta}{2})x = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ -i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix}$$

$$\begin{aligned} & \cos(\frac{\theta}{2})(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) - i\sin(\frac{\theta}{2})(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}) = \\ & = \left( \begin{pmatrix} \cos(\frac{\theta}{2}) & 0 \\ 0 & \cos(\frac{\theta}{2}) \end{pmatrix} \right) + \left( \begin{pmatrix} 0 & -i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & 0 \end{pmatrix} \right) = \\ & = \begin{pmatrix} \cos(\frac{\theta}{2}) & -i\sin(\frac{\theta}{2}) \\ i\sin(\frac{\theta}{2}) & \cos(\frac{\theta}{2}) \end{pmatrix} \end{aligned}$$

- Rotazione intorno all'asse delle  $y$ :

$$R_y(\theta) = e^{-i\frac{\theta}{2}y} = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)y = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix}$$

- Rotazione intorno all'asse delle  $z$ :

$$R_z(\theta) = e^{-i\frac{\theta}{2}z} = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)z = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix}$$

$$\begin{aligned} & \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} - i\sin\left(\frac{\theta}{2}\right) \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ & \left[ -i \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right] \\ & = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & -\sin\left(\frac{\theta}{2}\right) \\ \sin\left(\frac{\theta}{2}\right) & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \end{aligned}$$

$$\begin{aligned} & \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) \end{pmatrix} - i\sin\left(\frac{\theta}{2}\right) \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \\ & = \begin{pmatrix} -i\sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & i\sin\left(\frac{\theta}{2}\right) \end{pmatrix} \\ & = \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) - i\sin\left(\frac{\theta}{2}\right) & 0 \\ 0 & \cos\left(\frac{\theta}{2}\right) + i\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \\ & \boxed{e^{-i\frac{\theta}{2}}A = \cos\left(\frac{\theta}{2}\right)\mathbb{I} - i\sin\left(\frac{\theta}{2}\right)A} \\ & = \begin{pmatrix} e^{-i\frac{\theta}{2}} & 0 \\ 0 & e^{i\frac{\theta}{2}} \end{pmatrix} \end{aligned}$$

### Misurazione nella base $z$ e nella base $x$

Le due basi principali in cui si può effettuare una misura sono la base  $z$  e la base  $x$ , legate alla matrice di Pauli  $z$  e  $x$ .

La base  $z$  è costituita dagli autostati:  $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  e  $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ , questa è la base in cui lo spin è misurato lungo l'asse delle  $z$  della sfera di Bloch.

Se un qubit si trova in uno stato generico:  $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ , la misura nella base  $z$  dà come risultato:

- $|0\rangle$  con probabilità  $|\alpha|^2$ ;
- $|1\rangle$  con probabilità  $|\beta|^2$ ,

In base  $x$  c'è costituita dagli autostati della matrice di Pauli  $x$ :

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ |-> &= \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \end{aligned}$$

Se vogliamo misurare in questa base, dobbiamo:

1. Applicare l'operatore di Hadamard  $H$ , che trasforma la base  $x$  nella base  $z$ ;

2. Eseguire una misura standard nella base  $z$ ;

3. Interpretare il risultato:

- . Se otteniamo  $|0\rangle$  il qubit era nello stato  $|+\rangle$ ;
- . Se otteniamo  $|1\rangle$  il qubit era nello stato  $|-\rangle$ ;

Cosa significa scegliere una base di misura? Quando decidiamo di misurare in una base diversa, stiamo cambiando il "punto di vista" con cui osserviamo il qubit:

- misurare in base  $z$  significa chiedere: "il qubit è più vicino a  $|0\rangle$  o a  $|1\rangle$ ?"
- misurare in base  $x$  significa chiedere: "il qubit è più vicino a  $|+\rangle$  o a  $|-\rangle$ ?"

Vediamo 2 esempi generici per capire come funziona misurando prima in  $z$  e poi in  $x$ .

Consideriamo uno stato generico:  $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ :

Misuriamo in base  $z$ :

$$P_{(0)} = |\alpha|^2 \quad P_{(1)} = |\beta|^2 = 1 - |\alpha|^2$$

$\langle z \rangle = P_{(0)} - P_{(1)} \rightarrow$  è l'aspettazione di  $z$  è la differenza tra le probabilità di ottenere  $|0\rangle$  e  $|1\rangle$ .  
 ↴ valore medio

Misuriamo in base  $x$ :

1. Applichiamo Hadamard allo stato  $|1\rangle\rangle$  per ottenere una combinazione che vada bene per la base X ( $|0\rangle\rangle$  e  $|1\rangle\rangle$ ) non vanno bene perché noi vogliamo sapere se la misurazione si avvicina di più a  $|1\rangle\rangle$  o  $|0\rangle\rangle$  nel caso della base X e non a  $|0\rangle\rangle$  o  $|1\rangle\rangle$ .

l'operatore H agisce su  $|0\rangle\rangle$  e  $|1\rangle\rangle$  come segue:

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

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

Quindi applicando H allo stato  $|1\rangle\rangle$ :

$$H|1\rangle\rangle = \alpha \left[ \frac{1}{\sqrt{2}}(|0\rangle\rangle + |1\rangle\rangle) \right] + \beta \left[ \frac{1}{\sqrt{2}}(|0\rangle\rangle - |1\rangle\rangle) \right] = \frac{\alpha}{\sqrt{2}}(|0\rangle\rangle + |1\rangle\rangle) + \frac{\beta}{\sqrt{2}}(|0\rangle\rangle - |1\rangle\rangle) = \frac{\alpha}{\sqrt{2}}|0\rangle\rangle + \frac{\alpha - \beta}{\sqrt{2}}|1\rangle\rangle + \frac{\beta}{\sqrt{2}}|0\rangle\rangle - \frac{\beta}{\sqrt{2}}|1\rangle\rangle =$$

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

2. Eseguiamo la misurazione in base Z.

$$\begin{aligned} P(|0\rangle\rangle) &= \left| \frac{\alpha + \beta}{\sqrt{2}} \right|^2 = \frac{1}{2}(\alpha^2 + 2\alpha\beta + \beta^2) \\ P(|1\rangle\rangle) &= \left| \frac{\alpha - \beta}{\sqrt{2}} \right|^2 = \frac{1}{2}(\alpha^2 - 2\alpha\beta + \beta^2) \end{aligned}$$

$$\left. \begin{aligned} P(|0\rangle\rangle) - P(|1\rangle\rangle) &= \left( \frac{1}{2}(\alpha^2 + 2\alpha\beta + \beta^2) \right) - \left( \frac{1}{2}(\alpha^2 - 2\alpha\beta + \beta^2) \right) = \\ &= \frac{1}{2}\alpha^2 + \alpha\beta + \frac{1}{2}\beta^2 - \frac{1}{2}\alpha^2 + \alpha\beta - \frac{1}{2}\beta^2 = \alpha\beta + \beta\alpha \\ &= \langle X \rangle = \langle + \rangle \times \langle + \rangle \rightarrow \text{l'aspettazione di un operatore } X \end{aligned} \right\}$$

in uno stato quantistico  $|1\rangle\rangle$

### Teorema quantistico di non clonazione

Il teorema di non clonazione mostra che è impossibile creare una copia perfetta di uno stato quantistico sconosciuto.

**TEOREMA:** Siano X e Y due sistemi quantistici. Supponiamo che il sistema X si trovi in uno stato quantistico arbitrario  $|1\rangle\rangle$ , che vogliamo copiare nel sistema Y. Il teorema afferma che NON ESISTE un'operazione unitaria U che soddisfi  $U(|1\rangle\rangle \otimes |0\rangle\rangle) = |1\rangle\rangle \otimes |1\rangle\rangle$  per ogni possibile stato  $|1\rangle\rangle$  di X e per uno stato arbitrario  $|0\rangle\rangle$  di Y.

### Clifford gates

Il gruppo è composto da 3 gates: Hadamard, gate di fase S e il CNOT.

#### Hadamard

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

applicando H agli operatori di Pauli

$$H \cdot H = I$$

come segue, li trasforma in ulteriori  $\Rightarrow H \cdot Z \cdot H = X$

operatori di Pauli

$$H \cdot Y \cdot H = -Y$$

#### gate di fase S

$$S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix} = \sqrt{-1}$$

se applichiamo S agli operatori di

$$S \cdot S = I$$

Pauli quello che troviamo è

$$S \cdot Y \cdot S = -X$$

$$S \cdot Z \cdot S = Z$$

#### C-NOT

$$C\text{-NOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Un gate di Clifford con qubit multipli, trasformano un prodotto tensoriale di Pauli in un prodotto tensoriale di Pauli

$$C\text{-NOT} \cdot (X \otimes I) \cdot C\text{-NOT} = X \otimes X$$

$$C\text{-NOT} \cdot (I \otimes X) \cdot C\text{-NOT} = I \otimes X$$

$$C\text{-NOT} \cdot (Z \otimes I) \cdot C\text{-NOT} = Z \otimes Z$$

$$C\text{-NOT} \cdot (I \otimes Z) \cdot C\text{-NOT} = Z \otimes Z$$

Anche gli operatori di Pauli possono essere considerati dei gate di Clifford in quanto:

$$X \cdot Z \cdot X = -Z$$

$$X \cdot Y \cdot X = -Y$$

$$X \cdot X \cdot X = X$$

**Definizione Clifford gate:** Un operatore unitario U è un **Clifford gate** se, per ogni operatore di Pauli P, il suo effetto coniugato preserva la struttura di Pauli:  $U \cdot P \cdot U^\dagger \in \{\pm X, \pm Y, \pm Z, \pm I\}$

## NON-Clifford gate

Un Clifford gates può essere usato per espandere il potere dei non-Clifford gates, ad esempio possiamo cambiare la rotazione degli assi:  $U R_x(\theta) U^\dagger = e^{-i\theta U \times U^\dagger/2} \rightarrow H R_x(\theta) H = e^{i\theta H \times H/2} = e^{i\theta z/2} = R_z(\theta)$

## ALGORITMI

Molte porte logiche sono irreversibili, perché corrispondono a trasformare 2 bits in 1 solo e lo stato finale di un singolo qubit non permette di ricostituire lo stato iniziale di 2 bit. Ad esempio nel caso della porta logica XOR:

$$\begin{array}{l} 00 \xrightarrow{\text{XOR}} 0 \\ 01 \xrightarrow{\text{XOR}} 1 \\ 10 \xrightarrow{\text{XOR}} 1 \\ 11 \xrightarrow{\text{XOR}} 0 \end{array} \quad \left. \begin{array}{l} \text{da qui non è possibile} \\ \text{fare l'operazione inversa.} \end{array} \right\}$$

Ma in quantum computing non funziona allo stesso modo, perché qualsiasi computazione **irreversibile** è trasformabile in una **reversibile**.

Vediamo come possiamo trasformare la porta logica XOR in una equivalente in q.c.:

$$\begin{array}{l} 00 \xrightarrow{\text{CNOT}} 00 \\ 01 \xrightarrow{\text{CNOT}} 01 \\ 10 \xrightarrow{\text{CNOT}} 11 \\ 11 \xrightarrow{\text{CNOT}} 10 \end{array} \quad \left. \begin{array}{l} \text{d'operazione CNOT è equivalente allo XOR,} \\ \text{ma è anche possibile effettuare l'operazione al contrario.} \end{array} \right\}$$

### [ATTENZIONE!] Funzionamento CNOT

Abbiamo due bit  $x$  e  $y$ ,  $x$  viene chiamato controllo e  $y$  viene chiamato bersaglio.

A questo punto se il bit di controllo è pari a 1 il bit di bersaglio viene flippato (se è 0 viene posto a 1 e viceversa). Altrimenti se il controllo è pari a 0 non succede nulla, risiamo il bersaglio come l'ha trovato.

## Computazione quantistica reversibile

Un processo quantistico dovrebbe realizzare la trasformazione  $|x\rangle \rightarrow |f(x)\rangle = |f(x)\rangle$ , ovvero trasformare un input  $|x\rangle$  direttamente nel valore della funzione  $|f(x)\rangle$ . Tuttavia questo non è sempre possibile per qualsiasi funzione  $f(x)$ .

Infatti, le trasformazioni unitarie in meccanica quantistica conservano il prodotto scalare tra copie di stati. Questo significa che se esistono due stati  $|x_1\rangle \neq |x_2\rangle$  distinti tali che  $|f(x_1)\rangle = |f(x_2)\rangle$ , allora:  $\langle f(x_1)|f(x_2)\rangle = 1$ .

Ma per le proprietà delle trasformazioni unitarie, il prodotto scalare deve essere conservato e quindi:  $\langle x_1|x_2\rangle = \langle Ux_1|Ux_2\rangle$ . Se  $|x_1\rangle$  e  $|x_2\rangle$  sono ortogonali ( $\langle x_1|x_2\rangle = 0$ ), allora anche  $\langle Ux_1|Ux_2\rangle$  dovrà esserlo. Ma nel nostro caso abbiamo  $\langle f(x_1)|f(x_2)\rangle = 1$  il che **contraddice la condizione di unitarietà**.

Questo dimostra che una trasformazione del tipo  $|x\rangle \rightarrow |f(x)\rangle$  NON può essere realizzata in modo unitario.

### [ATTENZIONE!] Spiegazione: conservare il prodotto scalare tra copie di stati

Il prodotto scalare tra due stati quantistici  $|y\rangle$  e  $|z\rangle$  è indicato come  $\langle y|z\rangle$ , misura la loro "somiglianza" o sovrapposizione. Se due stati sono ortogonali (completamente diversi) il loro prodotto scalare è  $\langle y|z\rangle = 0$ .

Gli operatori unitari devono conservare questa proprietà. In altre parole, se abbiamo  $|x_1\rangle$  e  $|x_2\rangle$  e applichiamo ad entrambi  $U$ , i nuovi stati  $|Ux_1\rangle$  e  $|Ux_2\rangle$  avranno lo stesso prodotto scalare che avevano gli stati originali:

$$\langle x_1|x_2\rangle = \langle Ux_1|Ux_2\rangle$$

$$|x\rangle @ |y\rangle \rightarrow |Ux\rangle @ |y\rangle = |x\rangle @ |y\rangle + f(x)|y\rangle$$

→ rappresenta lo XOR

Per poter compiere un modo reversibile, si introduce un secondo registro, inizializzato in uno stato ausiliario  $|y\rangle$ . Il processo quantistico allora esegue la trasformazione:

**Importante:** questa formulazione permette di rendere la computazione reversibile.

Se inizializziamo il secondo registro a  $|y\rangle = |0\rangle$  allora l'operazione diventa:

$|x\rangle @ |0\rangle \rightarrow |x\rangle @ |f(x)\rangle$ . A questo punto se riinizializziamo il secondo registro (quello che conteneva  $y$ ), otteriamo direttamente  $|f(x)\rangle$ .

L'aspetto più potente della computazione quantistica è che possiamo preparare lo stato iniziale non come un singolo valore  $x$ , ma come una sovrapposizione di più stati contemporaneamente.

Ad esempio se applichiamo Hadamard  $H^m$  al primo registro inizializzato in  $|0\rangle^m$ , otteriamo una sovrapposizione uniforme di tutti i possibili ingressi:  $H^m|0\rangle^m = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} |n\rangle = \frac{1}{\sqrt{2^m}} (|0\rangle + |1\rangle) @ (|0\rangle + |1\rangle) @ \dots @ (|0\rangle + |1\rangle)$ . Ora, se

applichiamo la computazione reversibile delle funzioni  $f(x)$ , otteniamo:  $|1x\rangle \otimes |0\rangle = \frac{1}{\sqrt{2^m}} \sum_{n=0}^{2^m-1} |n\rangle \otimes |f(n)\rangle$ . Questo significa che il processore quantistico ha calcolato simultaneamente tutti i valori di  $f(n)$  per ogni possibile  $n$ , cioè tutti gli stati corrispondenti ai valori  $f(n)$  sono ora presenti nella sovrapposizione quantistica risultante.

### Phase Kick-Back

È un'effetto chiave che permette di trasferire informazioni sulla fase di un qubit di lavoro a un altro qubit di controllo. In altre parole, invece di cambiare direttamente la fase di un qubit target, l'effetto viene spinto indietro sul controllo.

Vediamo un esempio:

- Supponiamo di avere un qubit di **target** nello stato  $|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Il qubit **controllo** è nello stato  $|0\rangle$ , quindi abbiamo uno stato complessivo:  
 $|0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |0\rangle|1\rangle)$

- Ora applichiamo il CNOT che inverte il **target** solo se il **controllo** è pari a  $|1\rangle$ :

$$\text{CNOT}\left(\frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |0\rangle|1\rangle)\right) = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle - |0\rangle|1\rangle) \rightarrow |0\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

\* \* \* \* \*

- Supponiamo di avere un qubit di **target** nello stato  $|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$
- Il qubit **controllo** è nello stato  $|1\rangle$ , quindi abbiamo uno stato complessivo:  
 $|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}(|1\rangle|0\rangle - |1\rangle|1\rangle)$

- Ora applichiamo il CNOT che inverte il **target** solo se il **controllo** è pari a  $|1\rangle$ :

$$\text{CNOT}\left(\frac{1}{\sqrt{2}}(|1\rangle|0\rangle - |1\rangle|1\rangle)\right) = \frac{1}{\sqrt{2}}(|1\rangle|1\rangle - |1\rangle|0\rangle) \rightarrow |1\rangle \otimes \frac{1}{\sqrt{2}}(|1\rangle - |0\rangle) \rightarrow -|1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

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

Quindi generalizzando i due casi con un qubit di controllo pari a  $|x\rangle$  possiamo scrivere l'applicazione del CNOT con un qubit target pari a  $|y\rangle$  come:

$$\text{CNOT}(|x\rangle \otimes |y\rangle) = (-1)^x |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle), \text{ dove } x \in \{0, 1\}$$

Possiamo notare come la seconda applicazione del CNOT in cui il controllo era pari a  $|1\rangle$  abbia rimandato il cambiamento di fase solamente al qubit di controllo lasciando inalterato il qubit target.

### Quantum Teleportation

Possiamo trasferire lo stato quantistico di un qubit da un luogo ad un altro senza che il qubit stesso venga fisicamente trasportato.

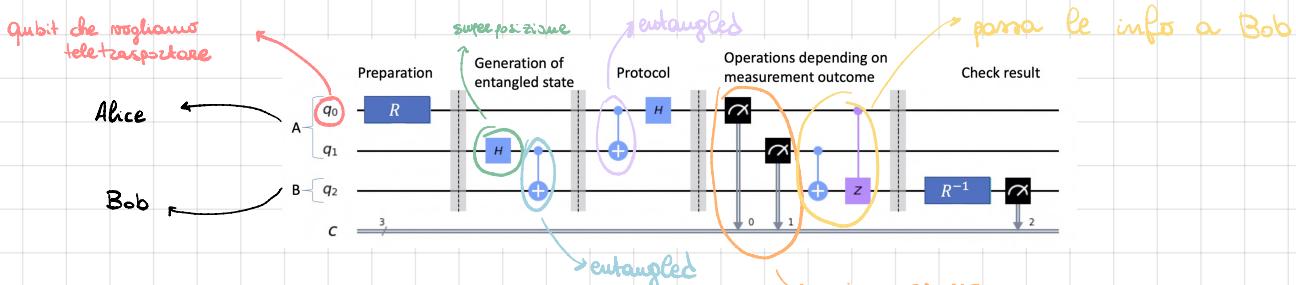
Per eseguire l'algoritmo abbiamo bisogno di 3 concetti fondamentali:

1. Entanglement
2. Comunicazione classica
3. Misura

Supponiamo che Alice voglia telescopiare lo stato di un qubit a Bob. Il circuito quantistico ha bisogno di 3 qubits. Alice mette il suo qubit in una superposizione con la porta di Hadamard e a questo punto mette il qubit in uno stato entangled con il qubit detenuto da Bob utilizzando una porta CNOT. Ora Alice detiene un ulteriore qubit ( $3^{\text{rd}}$ ) che ha lo stato che deve essere trasportato e lo pone entangled con il suo qubit iniziale. A questo punto Alice misura i suoi due qubit in due basi differenti, che distrugge le sue informazioni quantistiche ma le dà le informazioni classiche che deve fornire a Bob. Al ricevimento, Bob utilizza le informazioni classiche per eseguire operazioni sul suo qubit che poi gli consentono di utilizzare

lo stato quantistico telescopiato per qualsiasi scopo.

Quindi a livello di circuito abbiamo:



$$\begin{array}{l|l} q_0 = |1\rangle & \\ \hline q_1 = |0\rangle & H(q_1) = |+\rangle \\ q_2 = |0\rangle & \end{array}$$

$$\text{CNOT}(q_1, q_2) = |\Psi^+\rangle$$

$$\textcircled{1} \text{ CNOT}(q_0, q_1) = 11$$

$$H14 = 1 -$$

$$\text{CNOT}(q_1, q_2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

$$q_0 = 1 \rightarrow$$

$$H|10\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) = |+\rangle$$

$$\begin{aligned}
 CNOT(|1\rangle, |0\rangle) &= CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\otimes|0\rangle\right) = CNOT\left(\frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|0\rangle)\right) = \\
 &= \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) \quad (\text{state entangled}) = |10\rangle
 \end{aligned}$$

Supponiamo che si trovi in 10>

$$CNOT(q_0, q_1) = CNOT(11\rangle \otimes 10\rangle) = 12\rangle 11\rangle$$

$$H|12\rangle = \frac{1}{\sqrt{2}}(|10\rangle - |12\rangle) = |1-\rangle$$

$$\text{CNOT}(q_1, q_2) = \text{CNOT}(|1\rangle\langle 1| \otimes |0\rangle\langle 0|) = |1\rangle\langle 1|$$

$$\begin{aligned} Z(q_0, q_2) &= Z(1 \rightarrow 0 \otimes 12) = Z\left(\frac{1}{\sqrt{2}}(10 \rightarrow -12) \otimes 12\right) = Z\left(\frac{1}{\sqrt{2}}(10 \rightarrow 12 - 12 \rightarrow 12)\right) = \\ &= \frac{1}{\sqrt{2}}(10 \rightarrow 12 + 12 \rightarrow 12) \end{aligned}$$

# Superdense Coding

Permette di inviare 2 bit classici ad un altro utente utilizzando solamente un qubit.

## Teleportation vs Superdense

Ternary basis 1	Ternary basis 2
qubit utilization	c-bits utilization
2 c-bits	1 qubit

Alice vuole inviare 2 classici bit s utilizzando un solo qubit al destinatario Bob. In input al circuito abbiamo 2 qubit che mettono in uno stato entangled tra di loro. Alice deve inviare 2 bit classici B<sub>1</sub> e B<sub>2</sub>, agenda su un singolo suo qubit nel seguente modo:

- Se  $B_1 = B_2 = 0$  Alice lancia il qubit nello stato  $|0\rangle$
  - Se  $B_1 = 0$  e  $B_2 = 1$  allora Alice applica una porta X al suo qubit
  - Se  $B_1 = 1$  e  $B_2 = 0$  Alice applica una porta Z al suo qubit
  - Se  $B_1 = B_2 = 1$  Alice applica sia la porta Z che la X al suo qubit

Una volta applicata la porta corretta invia il suo qubit a Bob, ora Bob ha 2 qubit.

A questo punto Bob deve misurare entrambi i qubit capendo le combinazioni dei bit ( $B_1$  e  $B_2$ ).

### Deutsch-Josza

Permette, data una funzione booleana in input, di stabilire se questa è costante o bilanciata. La funzione viene considerata **costante** se gli output di questa sono tutti 0 oppure 1. La funzione è considerata **bilanciata** quando esattamente metà degli output sono pari a zero e l'altra metà è pari a 1.

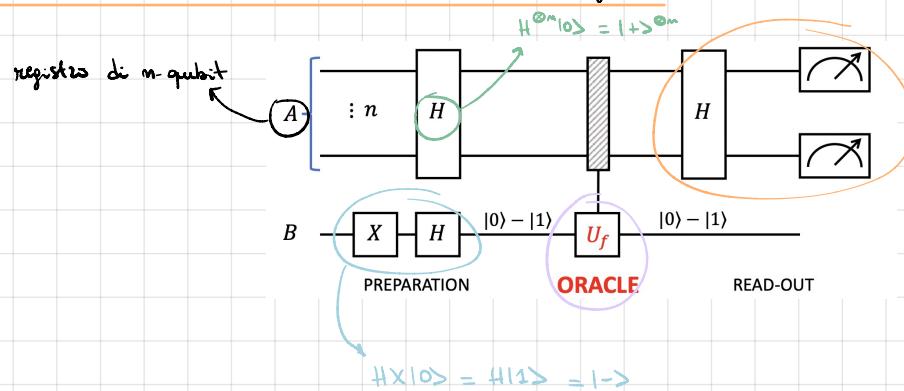
In un computer classico dobbiamo valutare la funzione un numero di volte esponenziale per avere un risultato certo, mentre con i computer quantistici basta una singola valutazione.

Abbiamo bisogno di 2 registri:

- 1) un registro di  $m$ -qubit inizializzato allo stato  $|+\rangle^{\otimes m} = H^{\otimes m}|0\rangle$  che chiameremo A;
- 2) un registro di un qubit inizializzato a  $|-\rangle = H|1\rangle$  che chiameremo B;

Successivamente definiamo l'**oracolo** come una black-box in cui avviene la trasformazione:  $|x\rangle_A|y\rangle_B \rightarrow |x\rangle_A|y\rangle_B f(x)$ .

Dopo di che' avviene una misurazione nella base X del primo register.



Possiamo l'algoritmo con  $m=1$ :

$$A = |0\rangle \text{ prepariamo lo stato} \rightarrow H|0\rangle = |+\rangle$$

$$B = |0\rangle \text{ prepariamo lo stato} \rightarrow H|0\rangle = H|1\rangle = |-\rangle$$

Applichiamo l'oracolo ai due stati:  $|x\rangle_A|y\rangle_B = |x\rangle_A \otimes |y\rangle \otimes f(x)|_B$

$$\left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] \otimes \left[ \frac{1}{\sqrt{2}} (|f(x)\rangle_B - |1-f(x)\rangle_B) \right] = \left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] \otimes \left[ (-1)^{f(x)} \frac{1}{\sqrt{2}} (|0\rangle_B - |1\rangle_B) \right]$$

$$= \frac{1}{2} [(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle]_A \otimes (|0\rangle - |1\rangle)_B \quad \xrightarrow{\text{costante se } f(0) = f(1)} \frac{1}{2} (|0\rangle + |1\rangle)_A \otimes (|0\rangle - |1\rangle)_B$$

$\hookrightarrow$  misurando A abbiamo

$$\text{la risposta } |0\rangle_A \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

bilanciato se  $f(0) \neq f(1)$

$$\frac{1}{2} (|0\rangle - |1\rangle)_A \otimes (|0\rangle - |1\rangle)_B$$

$\hookrightarrow$  misurando A abbiamo

$$\text{la risposta } |0\rangle_A \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

### Quantum Fourier Transform

La trasformata di Fourier classica, prende un insieme di valori nel dominio del tempo in un insieme equivalente nel dominio delle frequenze.

Per quanto riguarda i computer quantistici, QFT converte l'informazione **della base computazionale** in un'informazione **nella base di Fourier**, rendendo efficienti alcuni calcoli.

La QFT può essere implementata con una serie di porte quantistiche:

- Porta Hadamard (H): creano sovrapposizioni e distribuiscono le ampiezze di probabilità;
- Porta di fase controllata (CPhase): aggiungono i fattori di fase necessari per la trasformazione;

Come funziona?

1. Applica una porta H al primo qubit;
2. Applica porte di fase controllate tra il primo qubit e gli altri, con angoli di rotazione dipendenti dalla distanza tra i qubit;
3. Ripeti il processo per ogni qubit rimanente, applicando H e rotazioni di fase;
4. Alla fine applica permutazioni degli stati dei qubit per riorganizzare il risultato.

$$U_N^{\text{QFT}} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} e^{2\pi i x y / N} |y\rangle\langle x|$$

dove:  
 $|x\rangle$  è lo stato di input;  
 $N = 2^n$  è la dimensione dello spazio degli stati;  
 $e^{2\pi i x y / N}$  è il fattore di fase che codifica le informazioni sulle frequenze.

## ERROTI

Spesso non abbiamo abbastanza informazioni per specificare il vettore di stato di un sistema quantistico, ma conosciamo la probabilità  $P_m$  di trovarci in uno stato  $|q_m\rangle$ .

Nel caso in cui ci troviamo in uno stato puro di un sistema ad  $n$ -qubit esso è descritto da un vettore di stato  $|q\rangle$ . Tuttavia non tutti i sistemi quantistici si trovano in stati puri, in molte occasioni di situazioni reali, gli **stati sono misti**, cioè rappresentano una distribuzione probabilistica di stati puri.

Per trattare sistemi che si trovano in stati misti, come quelli affetti da rumore, ci viene in aiuto la **matrice densità** che viene definita nel seguente modo:

$$\rho = \sum_i P_i |q_{i,1}\rangle\langle q_{i,1}|$$

Se il sistema è in uno stato puro, quindi in un singolo stato  $|q\rangle$ , l'operatore di densità è:  $\rho = |q\rangle\langle q|$ . In questo caso,  $\rho$  è un proiettore e soddisfa la proprietà  $\text{Tr}(\rho^2) = 1$ .

Se il sistema è in una sovrapposizione di stati puri, con probabilità diverse, allora si è in un vero stato misto e la traccia di  $\rho^2$  soddisfa  $0 < \text{Tr}(\rho^2) < 1$ .

(esempio di stato misto: un sistema parzialmente entangled).

## Decrescenza quantistica

La decrescenza quantistica è un fenomeno fondamentale che descrive il processo attraverso il quale un sistema quantistico perde la sua coerenza a causa dell'interazione con l'ambiente esterno.

## Traccia parziale

Quando studio il comportamento del sistema quantistico mentre interagisce con l'ambiente esterno, spesso ci si concentra su un **sottosistema** più piccolo. Poiché non possiamo descrivere l'intero sistema dobbiamo ridurre la **descrizione** alla sola parte di interesse.

Matematicamente, questo si ottiene utilizzando la **traccia parziale** della matrice di densità del sistema totale. Se il sistema totale è descritto da  $\rho_{\text{tot}}$ , la matrice di densità ridotta del sottosistema è:  $\rho_{\text{sottosistema}} = \text{Tr}_{\text{ambiente}}(\rho_{\text{tot}})$ . Questa operazione nasconde le informazioni sullo stato dell'ambiente e fornisce una descrizione efficace dell'evoluzione del sistema di interesse.

Dato che con l'interazione con l'ambiente esterno introduce perdita di informazione, l'evoluzione del sistema non viene più descritta solo da operatori unitari. Invece, viene utilizzato più generale chiamato **operazione quantistica o superoperatore  $\mathcal{E}$**  che descrive l'evoluzione della matrice densità:  $\rho(t+1) = \mathcal{E}(\rho(t))$ .

↳  $\mathcal{E}$  è un'operazione positiva che utilizza le mappe di Kraus.

## Canale di Depolarizzazione

È un modello di rumore quantistico che descrive la perdita di informazioni in un sistema quantistico aperto.

Quando un qubit attraversa questo canale, c'è una probabilità  $p$  che il suo stato venga sostituito da uno stato completamente misto. Questo significa che il qubit perde gradualmente la sua informazione e tende a diventare un qubit casuale.

L'evoluzione della matrice di densità  $\rho$  sotto l'effetto del canale è descritta:  $E(\rho) = (1-p)\rho + p\frac{I}{2}$

$\hookrightarrow p_z = \text{probabilità di depolarizzazione}$

## Rilassamento

Il rilassamento è anche un fenomeno di perdita di informazione nei sistemi aperti, si manifesta in due forme:

- $T_1$ : perdita di polarizzazione dello stato eccitato;
- $T_2$ : perdita della sovrapposizione quantistica;

### Rilassamento $T_1$ (decadimento dell'energia)

Descrivere la transizione di un qubit dallo stato eccitato  $|1\rangle$  allo stato fondamentale  $|0\rangle$  a causa dell'interazione con l'ambiente.

La probabilità di rimanere in uno stato eccitato decresce esponenzialmente nel tempo secondo la legge:  $P_1(t) = P_1(0)e^{-t/T_1}$ , dove  $T_1$  è il tempo caratteristico di rilassamento.

### Decadenza $T_2$

Misura quanto velocemente un qubit perde la coerenza quantistica senza necessariamente perdere energia. Questo significa che anche se  $|1\rangle$  non passa a  $|0\rangle$ , può perdere la fase di sovrapposizione quantistica.

## Mitigazione degli errori

### 1) Errori di misurazione

Quando misuriamo uno stato potremmo trovare il valore sbagliato con una certa probabilità, ad esempio un qubit nello stato  $|0\rangle$  potrebbe essere misurato come  $|1\rangle$  e viceversa.

L'errore di misurazione può essere descritto da una matrice di calibrazione, che rappresenta le probabilità di errore nei risultati misurati.

$H = \begin{bmatrix} P(0|0) & P(0|1) \\ P(1|0) & P(1|1) \end{bmatrix}$ , dove  $P(x|y)$  è la probabilità di misurare  $x$  nel valore corrispondente  $y$ , se  $x=y$  allora stiamo valutando la probabilità di misurare correttamente quello stato. Se  $x \neq y$  allora stiamo valutando la probabilità di aver misurato erroneamente lo stato  $x$  come lo stato  $y$ .

Ad esempio, se il dispositivo ha un errore di misurazione del 5% possiamo avere la seguente matrice:

$$H = \begin{bmatrix} 0,95 & 0,05 \\ 0,05 & 0,95 \end{bmatrix}$$

Per correggere gli errori di misurazione possiamo applicare la matrice di calibrazione in questo modo:

$$H_{\text{corretto}} = H^{-1} H_{\text{misurato}}$$

[ATTENZIONE!] Inversione di una matrice

se  $\det(H) = 0$  allora  $H$  non è invertibile, altrimenti se  $\det(H) \neq 0$  allora lo è. Se  $H = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$  allora  $H^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

### 2) Errori di porta (gate)

Dovuti da imperfezioni nelle operazioni logiche sui qubit. Questi errori possono essere mitigati tramite una tecnica chiamata **estrapolazione a zero rumore**.

L'idea è quella di eseguire il circuito con diversi livelli di rumore e poi estrapolare il risultato che si otterebbe in assenza di rumore.

Una volta ottenuti tutti i risultati si esegue un'interpolazione matematica per ottenere il valore a zero rumore.

