Notazioni e definizioni

Bits

0 1

Un bit può essere in 2 stati.
Ogni sistema è un insieme finito di stati stabili e discreti

Qbits

$\alpha|0\rangle + \beta|1\rangle \quad \alpha, \beta \in \mathbb{C}$
$|\alpha|^2 + |\beta|^2 = 1$

Un Qbit può essere in stato $|0\rangle$ o $|1\rangle$ ma anche in sovrapposizione (superposizione) i.e. combinazione lineare di stati $|0\rangle$ e $|1\rangle$

Definizione Un Qbit è descritto da un vettore unitario $\in \mathbb{C}^2$ a meno di un fattore di fase.

Per convenzione prendiamo come base di $\mathbb{C}^2$

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad e \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

in cui $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. $|\alpha|^2 + |\beta|^2 = 1$

se "misuriamo" $|\psi\rangle$ otteniamo $|0\rangle$ con probabilità $|\alpha|^2$ e $|1\rangle$ con probabilità $|\beta|^2$.

Oss. Se moltiplichiamo $|\psi\rangle$ per $e^{i\varphi}$ (φ reale) troviamo uno stato non distinguibile da $|\psi\rangle$

Scrivendo $\alpha = \cos\frac{\vartheta}{2}$ $\beta = e^{i\varphi}\sin\frac{\vartheta}{2}$ (dato che $|\alpha|^2+|\beta|^2=1$)

$$|\psi\rangle = \cos\frac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\frac{\vartheta}{2}|1\rangle \quad , \vartheta,\varphi\in\mathbb{R}$$

in questo modo si ottiene un punto sulla sfera unitaria, la sfera di Bloch

Def Se $|\psi\rangle$ è un qbit rappresentato ~~da~~ con la sfera di Bloch, definiamo il vettore unitario $(\cos\varphi\sin\vartheta, \sin\varphi\sin\vartheta, \cos\vartheta)$ il vettore di Bloch dello stato $|\psi\rangle$.

Definizione Un sistema n-qbits è descritto da un vettore unitario in $\underbrace{\mathbb{C}^2\otimes\dots\otimes\mathbb{C}^2}_{n}$ ← spazio di 1 qbit

Se consideriamo su $\mathbb{C}^2$ la base $|0\rangle$ $|1\rangle$

la base per gli stati $\mathbb{C}^{2^{\otimes n}}$ è

$$|x_1\rangle\otimes|x_2\rangle\otimes\dots\otimes|x_n\rangle \quad \text{con } x_j\in\{0,1\}.$$

Notazione $|x_1\rangle \otimes \dots \otimes |x_n\rangle \equiv |x_1 \dots x_n\rangle \equiv |\underline{x}\rangle$

$|i\rangle \equiv \begin{pmatrix} 0 \\ \vdots \\ i \\ \vdots \\ 0 \end{pmatrix}$ $i = 0, \dots, n$

Es. $|0\rangle \otimes |1\rangle = (1,0) \otimes (0,1) = (0,1,0,0) \equiv |01\rangle \in \mathbb{C}^4$

Es. In un sistema con 3 qbits, $|\psi\rangle$ è un vettore unitario

$$|\psi\rangle = \alpha_{000}|000\rangle + \alpha_{001}|001\rangle + \alpha_{010}|010\rangle + \alpha_{100}|100\rangle +$$
$$+ \alpha_{011}|011\rangle + \alpha_{101}|101\rangle + \alpha_{110}|110\rangle + \alpha_{111}|111\rangle$$

$\sum |\alpha_{ijk}|^2 = 1$.

Def Una gate quantistica è un operatore $U: V \to W$ unitario. $U(\alpha|u\rangle + \beta|v\rangle) = \alpha U|v\rangle + \beta U|v\rangle$.

U può essere rappresentato da una matrice (che dipende dalla scelta delle basi di V e W) (ossia da una unica)

Struttura di spazio di Hilbert.

Definiamo il prodotto scalare standard su $\mathbb{C}^n$: se $|u\rangle = \sum u_i |i\rangle$ $|v\rangle = \sum v_i |i\rangle$

$$\langle u|v\rangle = \sum \overline{u_i} \cdot v_i \qquad \|u\| = \sqrt{\langle u|u\rangle}$$

$\langle u|$ - bra $\qquad |v\rangle$ - ket $\qquad \langle u|v\rangle$ braket

Prodotto esterno se V, W sv.

a $|u\rangle \in V$, $|v\rangle \in W$ associamo l'operatore lineare

$$(|u\rangle\langle v|) : W \longrightarrow V$$

$$(|u\rangle\langle v|)\,|w\rangle = \langle v|w\rangle\,|u\rangle$$

oss. se A operatore lineare

$$A = \sum_{ij} a_{ij}\,|i\rangle\langle j|$$

Notazioni, Richiami

A operatore lineare $A = \sum a_{ij} |i\rangle\langle j|$

A associato $\longrightarrow$ A^+ aggiunto $A^+ = (\overline{A})^t$

$$\langle v | Aw \rangle = \langle A^+ v, w \rangle$$

A unitario $\iff$ $AA^+ = A^+A = I$

A normale $\iff$ $AA^+ = A^+A$

Th. A normale $\iff$ A diagonalizzabile $\iff$ esiste una base ortonormale di $\mathbb{C}^n$ fatta di autovettori $\iff \exists\, U$ unitaria t.c. $U^+AU = D$ U unitaria

A Hermitiano $\iff$ $A = A^+$

Th A hermitiano $\iff$ gli autovalori sono reali

A unitario $\Rightarrow$ normale $\Rightarrow$ diagonalizzabile

$$\langle Au, Av \rangle = \langle u, v \rangle$$

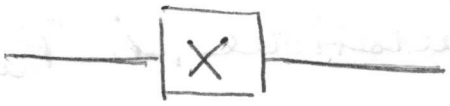
Conserva la norma -
Autovalori sono di modulo 1 -

Pauli Gates 1-qbits

$X|0\rangle = |1\rangle$

$X|1\rangle = |0\rangle$

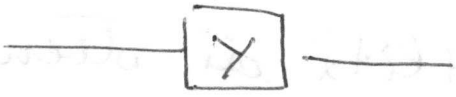
$\longleftrightarrow \quad X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ X-gate



$Y|0\rangle = i|1\rangle$

$Y|1\rangle = -i|0\rangle$

$\longleftrightarrow \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$ Y-gate



$Z|0\rangle = |0\rangle$

$Z|1\rangle = -|1\rangle$

$\longleftrightarrow \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ Z-gate

+ Identità.

Misurazione

Una misurazione su un sistema ha un insieme M di risultati.

Le misure sono descritte da $\{P_m \; m \in M\}$ di operatori di misurazione, i P_m sono operatori lineari unitari, che agiscono sullo spazio degli stati del sistema (spazio di Hilbert).

Se lo stato è $|\psi\rangle$ prima della misura allora la probabilità di ottenere m è

$$P(m) = \langle \psi | P_m^+ \cdot P_m | \psi \rangle = \| P_m |\psi\rangle \|$$

lo stato del sistema dopo la misura è

$$\frac{P_m |\psi\rangle}{\| P_m |\psi\rangle \|}$$

nota gli operatori P_m sono t.c. $\sum_{m \in M} P_m^+ P_m = I$

Con $\sum p(m) = \sum_m \langle \psi | P_m^+ \cdot P_m | \psi \rangle = \langle \psi | \psi \rangle = 1$

Es.

Misure nella base computazionale

Sono proiezioni su una base ortonormale.

per 1 qbit si prendono

$$P_0 = |0\rangle\langle 0| \qquad P_1 = |1\rangle\langle 1|$$

se $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ $\quad P_0|\psi\rangle = |\alpha|^2 \quad P_1|\psi\rangle = |\beta^2|$

Abbiamo già osservato che se da $|\psi\rangle$ consideriamo $e^{i\varphi}|\psi\rangle$, allora per ogni operatore unitario U

$$U e^{i\varphi}|\psi\rangle = e^{i\varphi} U|\psi\rangle$$

e qui per i P_m

$$\langle\psi| e^{-i\varphi} P_m^\dagger P_m e^{i\varphi}|\psi\rangle = \langle\psi| P_m^\dagger P_m$$

quindi una fase globale non è rilevabile

Se però ad es. consideriamo $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, che rispetto alla base comp. danno le stesse probabilità, e le misuriamo rispetto alla base $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ e $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ i risultati sono $\neq$

Se $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ $\quad H(|\psi_1\rangle) = |0\rangle \quad H|\psi_2\rangle = |1\rangle$.

fase rel

Un'ultima osservazione

Si è detto che un sistema composto è dato dal prodotto tensoriale dei singoli sistemi.

Uno stato di un sistema composto è <u>separabile</u> se è un tensore semplice ossia si può scrivere come prodotto tensoriale degli stati delle componenti

es.

$$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

ma

$$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \quad e \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

<u>non</u> possono essere separati. Questi stati si dicono <u>entangled</u>

Riassumendo:

1. Un sistema chiuso è descritto da un vettore unitario in uno spazio di Hilbert

*2. l'evoluzione di un sistema chiuso in un tempo finato è descritto da una matrice unitaria

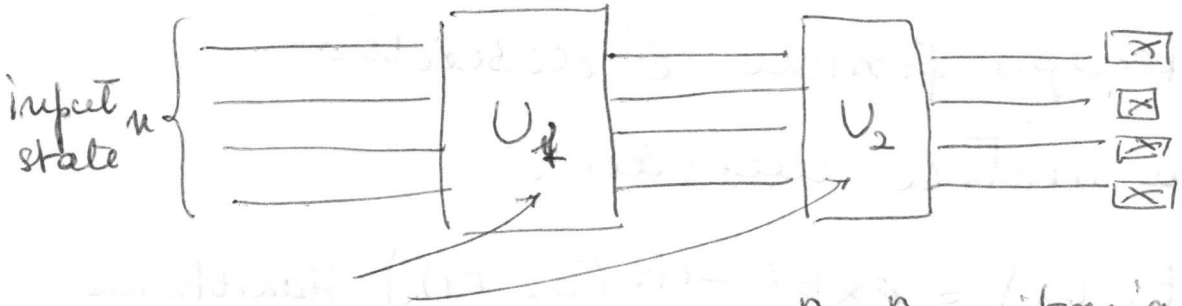
$$\left(U(t_1, t_2) = \exp\left(\frac{-iH(t_2 - t_1)}{\hbar} \right) \right.$$ Hamiltoniana del sistema)

3. Se misuriamo lo stato $|\psi\rangle$ in una base ortonormale $|0\rangle, |1\rangle \dots, |M-1\rangle$ otteniamo $|j\rangle$ con probabilità $|\langle j|\psi\rangle|^2$. Dopo la misura lo stato del sistema è il risultato della misura

4. Lo spazio degli stati di un sistema composto è il prodotto tensoriale degli spazi degli stati delle componenti

Come fare calcoli in questo modello?

modello di calcolo
Definiamo ~~un pacchetto~~ quantistico (quantum circuit) una successione di operazioni unitarie e di misure su uno stato di n-qbits.

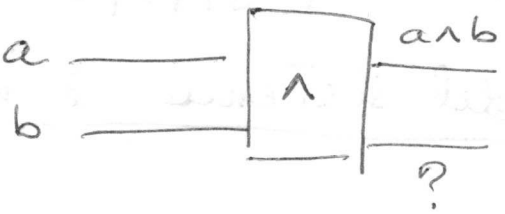


Vi matice $2^n \times 2^n$ unitaria.

Es. Simulare AND

a	b	a∧b
0	0	0
1	0	0
0	1	0
1	1	1

non può esistere operatore unitario!



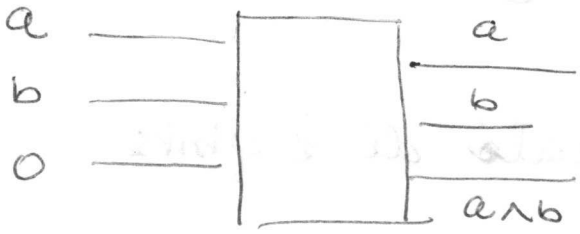
Non si possono perdere informazioni

Ogni operazione deve essere reversibile!

Es. Se $f: \{0,1\}^n \to \{0,1\}^m$ è una funzione Booleana la mappa $|x\rangle \to |f(x)\rangle$ può non essere unitaria - In questo caso implementiamo

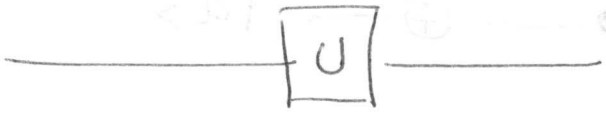
$$|x\rangle \otimes |0\rangle \longrightarrow |x\rangle \otimes |f(x)\rangle$$

Allora Aud. $f = \wedge$



ok!

Oss. (notazione) quando si scrive un circuito con un 1-qbit gate deve sempre essere visto come un'op. sull'intero stato



$U \otimes I$!

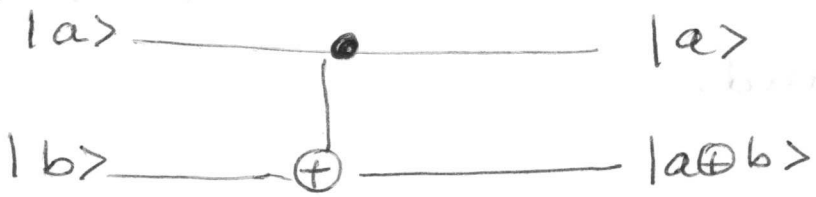
(non cambia l'esito della misurazione sul secondo bit)

Es CNOT gate – 2 qbits gate! è reversibile unitaria

a b	a CNOT b
0 0	0 0
0 1	0 1
1 0	1 1
1 1	1 0

$$C = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

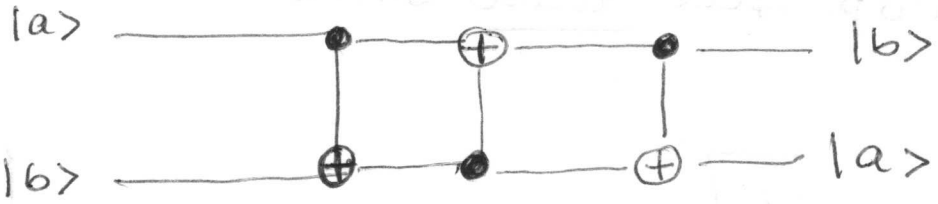
notazione



Es. Scambiare gli stati di 2 qbits

$$|a\,b\rangle \to |a, a\oplus b\rangle \to |a\oplus(a+b), a\rangle = |b, a\oplus b\rangle$$

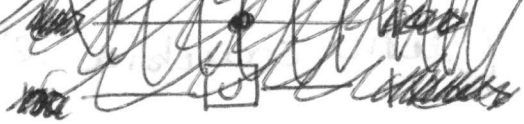
$$\to |b, (a\oplus b)\oplus b\rangle = |b, a\rangle$$



Logic gate.

Controlled U, U 1-qbit operators

Definiamo Controlled U gate

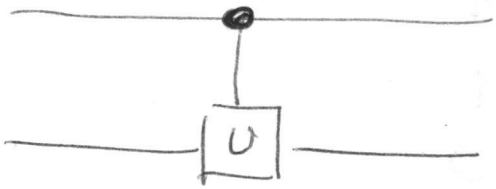


Convenzione Controlled U-gate (estende CNOT)

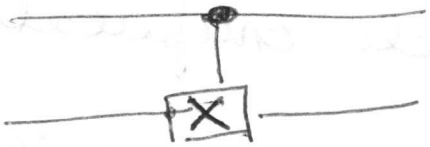
Se U è unitario su n qbits (targets)
aggiungiamo 1 qbit di controllo e otteniamo

$|0x\rangle \longrightarrow |0x\rangle$ se il 1° bit (di controllo = 0 nulla)

$|1x\rangle \longrightarrow |1Ux\rangle$ se 1 si applica U



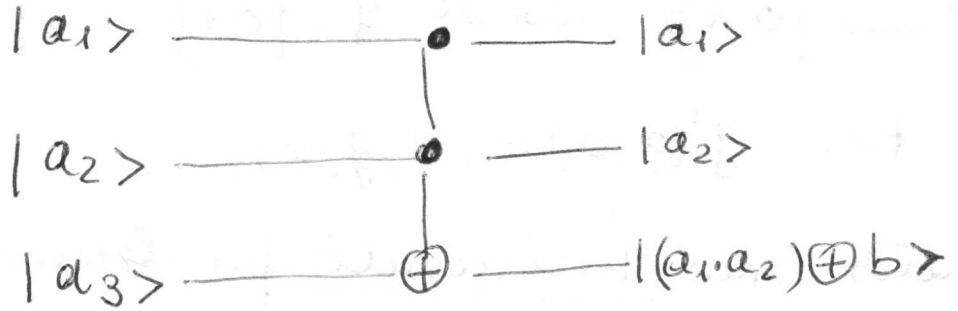
es. CNOT



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

GATE Molto importante: TOFFOLI GATE

3-qbits gate



Vale: Ogni matrice $2^n \times 2^n$ di permutazione può essere implementata usando SOLO Toffoligates

Toffoli.

input	output
0 0 0	0 0 0
0 0 1	0 0 1
0 1 0	0 1 0
0 1 1	0 1 1
1 0 0	1 0 0
1 0 1	1 0 1
1 1 0	1 1 1
1 1 1	1 1 0

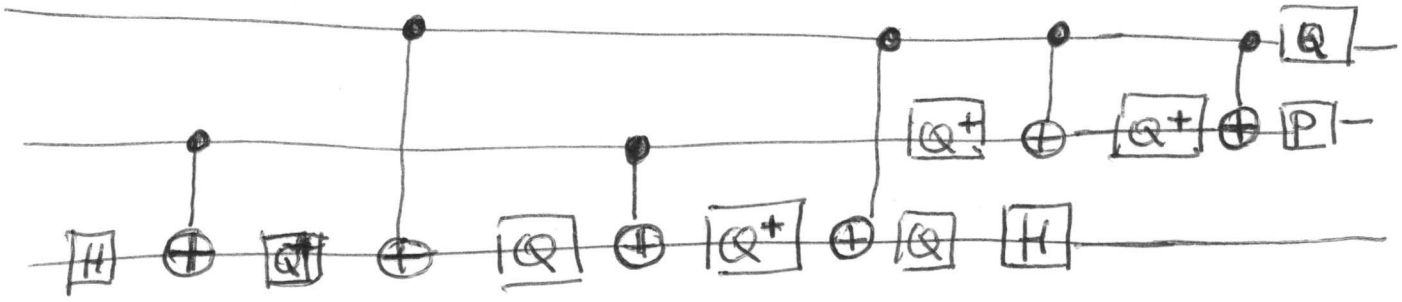
$$\left[\begin{array}{c|c} I_{6\times 6} & 0 \\ \hline & \begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix} \end{array}\right]$$

Classical reversible computation.

- $f: \{0,1\}^n \longrightarrow \{0,1\}^n$ è reversibile se è descritta da una matrice di permutazione $2^n \times 2^n$
- $\forall\, g: \{0,1\}^n \longrightarrow \{0,1\}^m$ esiste $g': \{0,1\}^{n+m} \longrightarrow \{0,1\}^{n+m}$ reversibile t.c. $g'(x,0) = (x, g(x))$
- I toffoli gates sono <u>universali</u> per ~~reversibile~~ computazioni reversibili i.e. $\forall$ funzione booleana f $\exists$ un circuito composto da TG che calcola f in modo reversibile.

Oss. Non è possibile implementare TG con 2 bit gates classici reversibili - Però:

TG Può essere implementato usando 2-qbit gg.



con $P=\begin{bmatrix}1&0\\0&i\end{bmatrix}$ $Q=\begin{bmatrix}1&0\\0&e^{i\pi/4}\end{bmatrix}$ $H=\frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix}$

GATES Universali

- Ogni operatore unitario su n bits può essere implementato come successione di 2-qbits operazioni
- Ogni operatore unitario può essere implementato con C-NOT e single qbit operazioni
- Ogni operatore unitario può essere approssimato a ogni grado di accuratezza richiesto usando solo C-NOT, H, P, Q.