UNIVERSITÀ DEGLI STUDI
DI GENOVA

Università degli Studi di Genova

Fondamenti di Computazione Quantistica

Lorenzo Vaccarecci

Anno Accademico 2024/2025

Indice

Capitolo 1

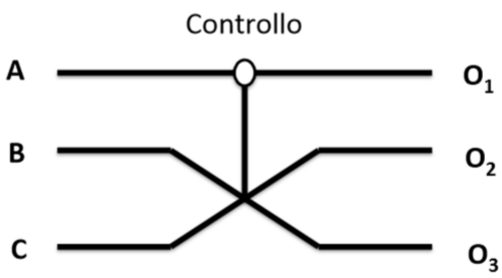
Fisica della computazione

1.1 Porte logiche universali

- `NOT(A)` $\equiv \bar{A}$
- `AND(A,B)` $\equiv A \cdot B$ oppure $A \wedge B$
- `OR(A,B)` $\equiv A + B$ oppure $A \vee B$
- `XOR(A,B)` $\equiv A \oplus B = (A + B) \mod 2$
- `NAND(A,B)` $\equiv A \bar{\cdot} B$ oppure $A \bar{\vee} B$
- `NOR(A,B)` $\equiv A \bar{+} B$ oppure $A \bar{\wedge} B$

L'insieme di `AND` e `NOT` oppure di `OR` e `NOT` sono insiemi universali. Questo significa che, ad esempio, usando solo combinazioni di porte `AND` e `NOT` è possibile implementare una qualsiasi funzione booleana. Pur formando set universali, le porte `AND`, `OR`, `NAND` e `NOR` sono però **irreversibili**. A livello concettuale è interessante introdurre delle porte logiche che siano **reversibili**. Questo vuol dire che se combiniamo in sequenza una porta logica reversibile con la sua inversa, riotteniamo l'informazione originale. La porta di Fredkin può essere interpretata come uno *switch* controllato di bit. Il bit di controllo è `A`; se questo è acceso i bit `B` e `C` vengono scambiati, altrimenti vengono lasciati identici.

A	B	C	Out1	Out2	Out3
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	1	0
1	1	0	1	0	1
1	1	1	1	1	1



1.2 Operazioni Bit-a-Bit

A una stringa di n bit possiamo associare un intero compreso fra 0 e $N-1$ con $N = 2^n$. All'intero x associamo la stringa di bit $x_0 x_1 x_2 \ldots x_n$ con $x_i = 0, 1$ e $i = 0, 1, \ldots, n$ tale che $x = \sum_{i=0}^{n} x_i 2^{n-i}$. Possiamo codificare $N = 2^n$ interi ma questi saranno compresi fra 0 e $N - 1 = 2^n - 1$.

1.2.1 Prodotto interno bit-per-bit

$$x \cdot z \equiv (x_1 z_1 + x_2 z_2 + \cdots + x_n z_n) \mod 2$$

E' anche chiamato prodotto `AND` bitwise perchè si ottiene prendendo le operazioni `AND` fra i singoli bit.

1.2.2 Somma bit-per-bit: bitwise `XOR`

Indichiamo con $x \oplus z$ la somma bit-per bit, modulo 2. Il risultato questa volta è una stringa il cui i-esimo bit ha il valore $x_i + z_i \mod 2 = x_i$ `XOR` z_i.

Capitolo 2

Apparato matematico

2.1 Prerequisiti matematici

2.1.1 Numeri complessi

Ogni numero complesso $z \in \mathbb{C}$ può essere scritto come $z = a + ib$, con $a \in \mathbb{R}$ **parte reale** e $b \in \mathbb{R}$ **parte immaginaria**. Se $z = a + ib$ e $w = c + id$, abbiamo

$$z + w = (a + c) + i(b + d)$$

$$z \cdot w = (ac - bd) + i(ad + bc)$$

Per ogni $z \in \mathbb{C}$, $z \cdot z^* = a^2 + b^2$ è reale e non negativo dove z^* è il **complesso coniugato** di z (la parte complessa è negata). Inoltre, $\sqrt{a^2 + b^2} = |z|$ è detto **modulo** di z.

$$|z|^2 = z \cdot z^*$$

Possiamo rappresentare un numero complesso $z = a + ib$ come una coppia (a,b) sul piano complesso. L'asse delle ascisse è utilizzato per la parte reale e l'asse delle ordinate per la parte immaginaria. Si ha $a = |z| \cos\theta$ e $b = |z| \sin\theta$ dove θ è la **fase**. Se $z = 0$ allora θ non è definita. Per $|z| = 1, z = \cos\theta + i \sin\theta$. Più in generale possiamo scrivere $z = pe^{i\theta}$ con $p = |z|$ e $e^{i\theta} = \cos\theta + i \sin\theta$.

$$i * (-i) = -1$$

2.1.2 Spazi vettoriali in 2D

- **Direzione**: rappresentata dalla retta su cui giace il vettore
- **Verso**: specifica in che direzione punta il vettore

Se abbiamo due vettori u e v possiamo definire la somma che sarà un vettore $w = u+v$ ottenuto mediante la **regola del parallelogramma**.
Dato un numero $\alpha \in \mathbb{R}$, per ogni vettore v, possiamo definire il vettore αv è la freccia ottenuta moltiplicando v per α in modulo e lasciando invariata la direzione se $\alpha > 0$ e invertendo il verso se $\alpha < 0$. Questa operazione è detta **moltiplicazione per scalare**. Se $\alpha = -1$, otteniamo il vettore $-v$ che ha stesso modulo, stessa direzione ma verso opposto a v.
L'insieme di tutti i vettori del piano è allora uno spazio vettoriale reale V chiuso rispetto all'operazione di combinazione lineare:

$$u = \alpha v + \beta w$$

Per ogni vettore u e $v \in V$ e per ogni $\alpha, \beta \in \mathbb{R}$.

2.1.3 Prodotto scalare e componenti

$$< \cdot, \cdot >: V \times V \to \mathbb{C}$$

Che soddisfa le seguenti proprietà:

1. $\forall u \in V, < u, u >$ è un numero reale non negativo, con $< u, u >= 0 \iff u = 0$
2. $\forall u, v \in V, < u, v >=< v, u >^*$
3. $\forall u, v, w \in V, \forall \alpha, \beta \in \mathbb{C}, < w, \alpha u + \beta v >= \alpha < w, u > +\beta < w, v >$

Due vettori per i quali il prodotto scalare è nullo sono *ortogonali*, sono base ortogonali se sono ortogonali e a norma unitaria ($\| < \cdot, \cdot > \|_2 = 1$).
Inoltre riscrivendo $u = u_0 v_0 + u_1 v_1$ si ha:

$$< u, u >=< u_0 v_0 + u_1 v_1, u_0 v_0 + u_1 v_1 >= u_0^2 + u_1^2$$

Dove $u_0 =< u, v_0 >$ e $u_1 =< u, v_1 >$

2.1.4 Vettori ket e bra

- **Ket**: vettore $u \to |u\rangle$
- **Bra**: vettore $u \to \langle u|$

Usando questa notazione il prodotto scalare si forma con *braket*:

$$< u, v >= \langle u|v\rangle$$

Usando la scomposizione di v in componenti:

- $|v\rangle = u_0|v_0\rangle + u_1|v_1\rangle$
- $\langle v| = u_0^*\langle v_0| + u_1^*\langle v_1|$

Delta di Kronecker

$$< v_i, v_j >= \delta_{ij} = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

Usando queste notazioni possiamo scrivere il prodotto scalare come:

$$\begin{aligned}
\langle v|v\rangle &= (u_0^*\langle v_0| + u_1^*\langle v_1|) \cdot (u_0|v_0\rangle + u_1|v_1\rangle) \\
&= |u_0|^2\langle v_0|v_0\rangle + u_0^* u_1\langle v_0|v_1\rangle + u_1^* u_0\langle v_1|v_0\rangle + |u_1|^2\langle v_1|v_1\rangle \\
&= |u_0|^2 \cdot 1 + u_0^* u_1 \cdot 0 + u_1^* u_0 \cdot 0 + |u_1|^2 \cdot 1 \\
&= |u_0|^2 + |u_1|^2 \\
&= ||v\rangle|^2
\end{aligned}$$

2.1.5 Prodotto tensore

Consideriamo ora due spazi vettoriali V e W con basi, rispettivamente, $A = \{|\alpha_1\rangle_V, \ldots, |\alpha_n\rangle_V\}$ e $B = \{|\beta_1\rangle_W, \ldots, |\beta_m\rangle_W\}$. Da questa scrittura deduciamo che V è uno spazio vettoriale di dimensione n e W di dimensione m.
Il prodotto tendore di V e W viene indicato con $V \otimes W$ ha dimensione $\dim(V \otimes W) = n\ m$ con la base costituita da $n\ m$ elementi della forma $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W$.
La notazione $|\alpha_i\rangle_V \otimes |\beta_j\rangle_W$ può essere scritta come $|\alpha_i\beta_j\rangle$.
Proprietà:

1. $\forall |v\rangle, |v'\rangle \in V, |w\rangle \in W \quad (|v\rangle + |v'\rangle) \otimes |w\rangle = |v\rangle \otimes |w\rangle + |v'\rangle \otimes |w\rangle$
2. $\forall |v\rangle \in V, |w\rangle, |w'\rangle \in W \quad |v\rangle \otimes (|w\rangle + |w'\rangle) = |v\rangle \otimes |w\rangle + |v\rangle \otimes |w'\rangle$
3. $\forall |v\rangle \in V, |w\rangle \in W, \alpha \in \mathbb{C} \quad (\alpha|v\rangle) \otimes |w\rangle = |v\rangle \otimes (\alpha|w\rangle) = \alpha(|v\rangle \otimes |w\rangle)$

Se V e W ammettono prodotto scalare, allora $V \otimes W$ ammette un prodotto scalare definito come:

$$\langle u|u'\rangle = (\langle v| \otimes \langle w|) \cdot (|v'\rangle \otimes |w'\rangle) = \langle v|v'\rangle \cdot \langle w|w'\rangle \in \mathbb{C}$$

Alcune "proprietà":

1. $(\langle\alpha_1| \otimes \langle\beta_2|) \cdot (|\alpha_1\rangle \otimes |\beta_2\rangle) = \langle\alpha_1|\alpha_1\rangle \cdot \langle\beta_2|\beta_2\rangle = 1$
2. $\{|\alpha_i\rangle \otimes |\beta_j\rangle\}$ è una base ortonormale $V \otimes W$
   - Se $\langle\alpha_i|\alpha_k\rangle \cdot \langle\beta_j|\beta_l\rangle = 1 \to$ normalizzati
   - Se $\langle\alpha_i|\alpha_k\rangle \cdot \langle\beta_j|\beta_l\rangle = 0 \to$ ortogonali

Esempio

$|v\rangle = a|\alpha_1\rangle_V + b|a_2\rangle_V \in V$
$|w\rangle = c|\beta_1\rangle_W + d|\beta_2\rangle_W \in W$

$$\begin{aligned}
|v\rangle \otimes |w\rangle &= (a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W) \\
&= ac(|\alpha_1\rangle_V \otimes |\beta_1\rangle_W) + ad(|\alpha_1\rangle_V \otimes |\beta_2\rangle_W) + bc(|\alpha_2\rangle_V \otimes |\beta_1\rangle_W) + bd(|\alpha_2\rangle_V \otimes |\beta_2\rangle_W) \\
\langle v| \otimes \langle w| &= (a\langle\alpha_1|_V + b\langle\alpha_2|_V) \otimes (c\langle\beta_1|_W + d\langle\beta_2|_W) \\
&= ac(\langle\alpha_1|_V \otimes \langle\beta_1|_W) + ad(\langle\alpha_1|_V \otimes \langle\beta_2|_W) + bc(\langle\alpha_2|_V \otimes \langle\beta_1|_W) + bd(\langle\alpha_2|_V \otimes \langle\beta_2|_W)
\end{aligned}$$

$$\begin{aligned}
(\langle v| \otimes \langle w|) \cdot (|v\rangle \otimes |w\rangle) &= [(a\langle\alpha_1|_V + b\langle\alpha_2|_V) \otimes (c\langle\beta_1|_W + d\langle\beta_2|_W)] \cdot [(a|\alpha_1\rangle_V + b|\alpha_2\rangle_V) \otimes (c|\beta_1\rangle_W + d|\beta_2\rangle_W)] \\
&= \\
&= (|a|^2 + |b|^2) \cdot (|c|^2 + |d|^2)
\end{aligned}$$

2.1.6 Operatori lineari

Gli operatori lineari in generale sono tali che agendo su un vettore dello spazio lineare danno un altro vettore dello stesso spazio: $O : V \to V$. Usando la notazione braket possiamo scrivere

$$O|v\rangle = |w\rangle$$

Scegliamo una base (ortonormale) dello spazio vettoriale $\{|\alpha_1\rangle, \ldots, |\alpha_n\rangle\}$, l'elemento della matrice O in posizione (i, j) sarà $O_{ij} = \langle\alpha_i| \cdot (O|\alpha_j\rangle)$

Esempio

Voglio calcolare O_{12}:

$$\begin{aligned} O_{12} &= \langle\alpha_1| \left(\sum_{ij}^{n} O_{ij} |\alpha_i\rangle\langle\alpha_j| \right) |\alpha_2\rangle \\ &= \sum_{ij}^{n} O_{ij} \langle\alpha_1|\alpha_i\rangle\langle\alpha_j|\alpha_2\rangle \\ &= O_{12} \end{aligned}$$

Grazie al delta di Kronecker.

2.1.7 Autovalori e Autovettori

Diremo che se $O|v\rangle = \lambda|v\rangle$ per un vettore non nullo $|v\rangle$, diremo che v è un **autovettore** di O e λ è l'**autovalore** corrispondente.

Capitolo 3

Introduzione ai fenomeni quantistici

Un osservabile fisico può essere associato ad un operatore Hermittiano ϕ da cui possiamo ottenere i loro autovalori e autovettori. Il punto fondamentale di questa discussione è che la base, gli autovalori e il risultato dipende dall'osservabile che vogliamo misurare.

3.1 Regole dal postulato della misura

1. Se vogliamo misurare un osservabile ϕ, dobbiamo conoscere i suoi autovalori $\{\phi_i\}$ e autovettori $\{|\phi_i\rangle\}$; cioè gli stati tali che $\phi|\phi_i\rangle = \phi_i|\phi_i\rangle$. Gli autovettori saranno la base su cui decomporre lo stato del nostro sistema. Ovvero dobbiamo scrivere $|a\rangle = \sum_i a_i|\phi_i\rangle$ con $a_i = \langle\phi_i|a\rangle$.
2. La misura avrà come risultato l'autovalore ϕ_i con probabilità $|a_i|^2$.
3. Dopo la misura, il sistema si troverà nello stato $|\phi_i\rangle$ associato all'autovalore misurato.

Stati quantistici sono normalizzati:

$$\sum_{i=1}^{N} |a_i|^2 = 1$$

3.2 Fase globale e relativa

3.2.1 Fase globale

Consideriamo i vettori $|u\rangle$ e $e^{i\phi}|u\rangle$ che hanno lo stesso modulo ma differiscono per una fase globale ϕ. Il calcolo delle probabilità dei risultati di una qualunque misura fornisce sempre gli stessi valori.
Sia $|u\rangle \sum_i \alpha_i|\phi_i\rangle$ dove $\{|\phi_i\rangle\}$ formano una base ortonormale dello spazio vettoriale. Lo stato con una fase globale si scriverà $e^{i\phi}|u\rangle = \sum_i e^{i\phi}\alpha_i|\phi_i\rangle$

Esempio di fase globale/relativa

$$\underset{\substack{\uparrow \\ \text{Fase globale}}}{e^{i\phi}} \frac{(|0\rangle + \overset{\substack{\text{Fase relativa} \\ \downarrow}}{e^{i(\gamma-\phi)}}|1\rangle)}{\sqrt{2}}$$

3.3 Stati a molti qubit

- **Base del qubit**: $\{|0\rangle, |1\rangle\}$
- **Stato**: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Consideriamo:

$$\begin{aligned} &\text{A: } |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \\ &\text{B: } |\phi\rangle = \gamma|0\rangle + \delta|1\rangle \end{aligned} \tag{3.1}$$

La base B la otteniamo con:

$$\begin{aligned} |\psi\rangle \oplus |\phi\rangle &= (\alpha|0\rangle + \beta|1\rangle) \oplus (\gamma|0\rangle + \delta|1\rangle) \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle \end{aligned}$$

Per ricavare la base ci fermiamo al secondo passaggio, quindi avremo $B : \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

3.3.1 Stati a due qubit separabili

Usando $|\psi\rangle$ e $|\phi\rangle$ (3.1), a volte conviene scrivere lo stato come:

$$|\psi\rangle \oplus |\phi\rangle = \alpha|0\rangle \oplus (\gamma|0\rangle + \delta|1\rangle) + \beta|1\rangle \oplus (\gamma|0\rangle + \delta|1\rangle)$$

Perchè in questo modo si possono determinare le probabilità di collasso in modo più semplice:

$$\begin{cases} \text{Se collassa } \alpha\text{: } |\alpha|^2, \phi_0 \to |0\rangle \oplus (\gamma|0\rangle + \delta|1\rangle) = \begin{cases} \text{Se collassa } \gamma\text{: } |\gamma|^2, \phi_0 \to |00\rangle \\ \text{Se collassa } \delta\text{: } |\delta|^2, \phi_1 \to |01\rangle \end{cases} \\ \text{Se collassa } \beta\text{: } |\beta|^2, \phi_1 \to |1\rangle \oplus (\gamma|0\rangle + \delta|1\rangle) = \begin{cases} \text{Se collassa } \gamma\text{: } |\gamma|^2, \phi_0 \to |10\rangle \\ \text{Se collassa } \delta\text{: } |\delta|^2, \phi_1 \to |11\rangle \end{cases} \end{cases}$$

Esempio

$$\begin{aligned} |\varepsilon\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)? = |\psi\rangle \oplus |\phi\rangle \\ &= \frac{1}{\sqrt{2}}(|01\rangle) + \frac{1}{\sqrt{2}}(|10\rangle) = \begin{cases} \text{Se collassa } |01\rangle\text{: } \frac{1}{2}, \phi_0 \to |01\rangle \to 1, \phi_0 \to |01\rangle \\ \text{Se collassa } |10\rangle\text{: } \frac{1}{2}, \phi_1 \to |10\rangle \to 1, \phi_1 \to |10\rangle \end{cases} \end{aligned}$$

Possiamo dedurre che se A misura 0, B misura 1 e viceversa.

3.3.2 Stati a due qubit entangled

Gli elementi dello spazio vettoriale $A \oplus B$ non sono tutti ottenibili come prodotto tensoriale di due elementi di A e B.
Un esempio di stati entangled sono gli stati di Bell:

$$\begin{aligned} |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \oplus |0\rangle_B + |1\rangle_A \oplus |1\rangle_B) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \oplus |0\rangle_B - |1\rangle_A \oplus |1\rangle_B) \\ |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \oplus |1\rangle_B + |1\rangle_A \oplus |0\rangle_B) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle_A \oplus |1\rangle_B - |1\rangle_A \oplus |0\rangle_B) \end{aligned}$$

Per descrivere lo stato di un sistema a due qubit possiamo alternativamente usare la base canonica $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ o la base di Bell $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$.

$$O = \lambda_0|\phi^+\rangle\langle\phi^+| + \lambda_1|\phi^-\rangle\langle\phi^-| + \lambda_2|\psi^+\rangle\langle\psi^+| + \lambda_3|\psi^-\rangle\langle\psi^-|$$

Quindi se il sistema si trova in uno stato di Bell, una misura dell'operatore O darà con certezza l'autovalore corrispondente.

3.4 Trasformazioni unitarie

Sia $|a\rangle = \alpha|x_0\rangle + \beta|x_1\rangle$, una trasformazione unitaria U è

- **Lineare**: $U|a\rangle = U(\alpha|x_0\rangle + \beta|x_1\rangle) = \alpha U|x_0\rangle + \beta U|x_1\rangle$
- **Invertibile con l'inversa uguale alla trasposta coniugata**: $U^{-1}|a\rangle = U^\dagger|a\rangle$

Quest'ultima proprietà garantice che le trasformazioni unitarie laasciano invariati i prodotti scalari, e quindi anche la norma dei vettori su cui agiscono e le probabilità associate alle misure. Infatti, prendiamo due stati $|a\rangle$ e $|b\rangle$ con prodotto scalare $\langle b|a\rangle$. Se questi evolvono secondo un operatore unitario U avremo $|a'\rangle = U|a\rangle$ e $|b'\rangle = U|b\rangle$ ($\langle b'| = \langle b|U^\dagger$), il prodotto scalare degli stati evoluti sarà $\langle b'|a'\rangle = \langle b|U^\dagger U|a\rangle = \langle b|a\rangle$ perchè $U^\dagger U =$ Identità.

3.4.1 Porte quantistiche

Trasformazioni di Pauli

Nel nostro caso scegliamo la base canonica $\{|0\rangle, |1\rangle\}$ e definiamo, oltre all'identità Id, le tre trasformazioni di Pauli X, Y, Z:

$$\begin{array}{rclrcl} Id|0\rangle & := & |0\rangle & Id|1\rangle & := & |1\rangle \\ X|0\rangle & := & |1\rangle & X|1\rangle & := & |0\rangle \\ Y|0\rangle & := & -i|1\rangle & Y|1\rangle & := & i|0\rangle \\ Z|0\rangle & := & -|0\rangle & Z|1\rangle & := & |1\rangle \end{array}$$

Analizzando l'effetto degli operatori, si nota che nella base canonica, X corrisponde al `NOT` tra bit classici. L'operatore Z genera un cambio della fase relativa e, infine, l'operatore Y può essere visto come una combinazione dei due precedenti dato che $Y = -iXZ$.

Esempio

$$\begin{aligned} Z(\alpha|0\rangle + \beta|1\rangle) &= \alpha Z|0\rangle + \beta Z|1\rangle \\ &= -\alpha|0\rangle + \beta|1\rangle \end{aligned}$$

Trasformazioni di Hadamard

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

In forma matriciale (nella base canonica $\{|0\rangle, |1\rangle\}$) l'operatore di Hadarmard si scrive come:

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

Controlled-NOT

Consideriamo ora, il controlled-NOT, `CNOT`, una trasformazione che agisce su 2 qubit, A e B. Nella base canonica l'azione del `CNOT` é:

$$\begin{aligned} CNOT|0\rangle_A \oplus |0\rangle_B &= |0\rangle_A \oplus |0\rangle_B \\ CNOT|0\rangle_A \oplus |1\rangle_B &= |0\rangle_A \oplus |1\rangle_B \\ CNOT|1\rangle_A \oplus |0\rangle_B &= |1\rangle_A \oplus |1\rangle_B \\ CNOT|1\rangle_A \oplus |1\rangle_B &= |1\rangle_A \oplus |0\rangle_B \end{aligned}$$

In linea generale possiamo scrivere il `CNOT` come:

$$C_i NOT_j$$

Dove i è il qubit di controllo e j il qubit target. Se il qubit di controllo è acceso allora applica un `NOT` al qubit target.
L'importanza dell'operatore `CNOT` risiede nel fatto che può generare entanglement fra due qubit.
Esempio

$$|00\rangle \xrightarrow{H_1} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \oplus |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xrightarrow{C_1NOT_2} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \text{Stato di Bell}$$

Se eseguo l'operatore `CNOT` due volte ottengo lo stato iniziale: $$CNOT^2 = Id$$

3.5 Sfera di Bloch

Come detto un generico stato quantistico a due livelli o qubit è scritto come $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ con il vincolo ulteriore di normalizzazione dello stato: $|\alpha|^2 + |\beta|^2 = 1$. Quindi in generale possiamo scrivere $|\alpha|^2 = \cos^2(\theta) \to |\alpha| = \cos\left(\frac{\theta}{2}\right)$ e $|\beta|^2 = \sin^2(\theta) \to |\beta| = \sin\left(\frac{\theta}{2}\right)$ Possiamo rappresentare gli stati dei qubit in modo geometrico. Consideriamo lo stato generico

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \sin\left(\frac{\theta}{2}\right)e^{i\phi}|1\rangle$$

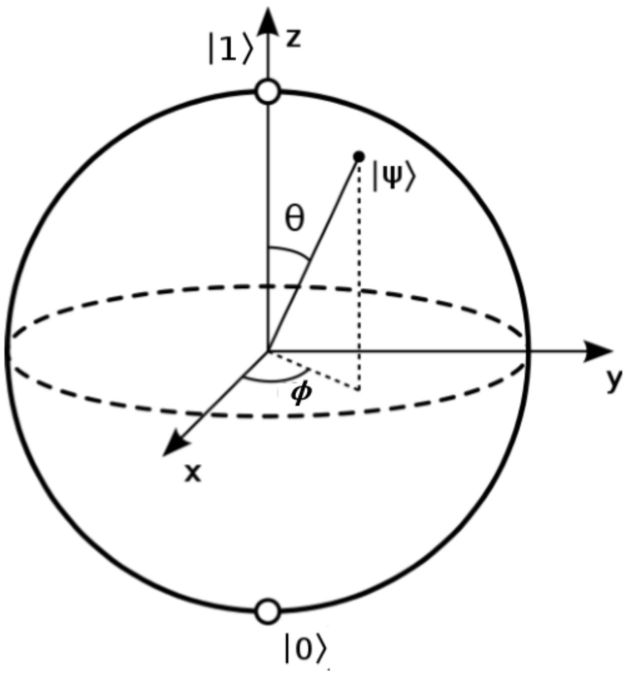
e il relativo stato bra

$$\langle\psi| = \cos\left(\frac{\theta}{2}\right)\langle 0| + \sin\left(\frac{\theta}{2}\right)e^{-i\phi}\langle 1|$$

Calcoliamo i valori medi degli operatori di Pauli X, Y, Z con lo stato $|\psi\rangle$

$$\begin{aligned} x &= \langle\psi|X|\psi\rangle = \cos\phi\sin\theta \\ y &= \langle\psi|Y|\psi\rangle = \sin\phi\sin\theta \\ z &= \langle\psi|Z|\psi\rangle = \cos\theta \text{ (oppure } -\cos\theta) \end{aligned}$$

Queste non sono altro che le coordinate in uno spazio tridimensionale di un punto che si muove su una sfera. Se consideriamo il vettore che congiunge l'origine degli assi con il punto di coordinate $\{x, y, z\}$, l'angolo θ è quello formato dal vettore e dall'asse z mentre l'angolo ϕ è quello formato dal vettore sul piano $y - z$



Concludiamo che ogni operatore unitario può essere visto come una rotazione sulla sfera di Bloch che unisce lo stato iniziale con lo stato finale.
L'operatore U possiamo scriverlo più generalmente come:

$$U = \cos\left(\frac{\alpha}{2}\right) Id - i \sin\left(\frac{\alpha}{2}\right) Y$$

Esempio

$$\begin{aligned}
|\psi\rangle &= |1\rangle \\
|\psi_f\rangle &= U|\psi\rangle \\
&= \cos\left(\frac{\alpha}{2}\right) Id|1\rangle - i \sin\left(\frac{\alpha}{2}\right) Y|1\rangle \\
&= \cos\left(\frac{\alpha}{2}\right) |1\rangle - i \sin\left(\frac{\alpha}{2}\right) i|0\rangle \\
&= \cos\left(\frac{\alpha}{2}\right) |1\rangle + \sin\left(\frac{\alpha}{2}\right) |0\rangle
\end{aligned}$$