Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

Lezione 2: Introduzione generale

1 Interpretazione geometrica di un qubit

Dimostriamo che un qubit

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

corrisponde a un punto sulla sfera unitaria in $\mathbb{R}^3$ rappresentato come

$$\cos(\theta/2) |0\rangle + e^{i\varphi} \sin(\theta/2) |1\rangle ,$$

dove θ e φ sono numeri reali (le coordinate sferiche del punto).

Questa sfera è nota come la sfera di Bloch (cf. Figura 1) e permette di visualizzare lo stato di un qubit. Molte delle operazioni su un singolo qubit che studieremo possono essere descritte all'interno di questa sfera, che ci aiuta così a coglierne il significato intuitivo.

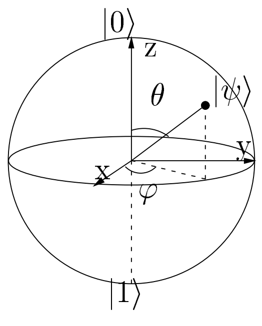

Figure 1: La sfera di Bloch

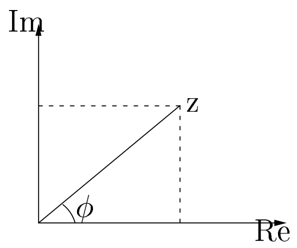

Figure 2: Il piano complesso: $z = a + ib$

Preliminari

Un numero complesso $z \in \mathbb{C}$ si può vedere come un punto nel piano complesso in Figura 2.

Due rappresentazioni equivalenti di z come punto in questo piano sono:

Coordinate cartesiane: z è il punto di coordinate a (sull'asse reale Re) e b (sull'asse immaginario Im), cioè $z = a + ib$, con $a, b \in \mathbb{R}$.

Coordinate polari: se ϕ è l'angolo che il vettore z forma con l'asse Re e $r = \sqrt{a^2 + b^2}$ è la norma di z, allora $a = r\cos(\phi)$ e $b = r\sin(\phi)$. Quindi z è indivuato dalle coordinate (r, ϕ), cioè $z = r(\cos(\phi) + i\sin(\phi)$. Dalla formula di Eulero

$$e^{i\phi} = \cos(\phi) + i\sin(\phi),$$

si ottiene quindi la rappresentazione di z come $re^{i\phi}$.

Ampiezze di un qubit

In un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, i valori α e β sono numeri complessi tali che $|\alpha|^2 + |\beta|^2 = 1$. Usando la descrizione di α e β in coordinate polari possiamo scrivere $|\psi\rangle$ come

$$|\psi\rangle = r_0 e^{i\phi_0}|0\rangle + r_1 e^{i\phi_1}|1\rangle,$$

con

$$r_0^2 + r_1^2 = 1. \tag{1}$$

Notiamo che l'equazione (1) descrive i punti del cerchio unitario in $\mathbb{R}^2$ (cf. Figura 3). Possiamo quindi rappresentare i moduli di α e β mediante l'angolo ρ, ponendo

$$r_0 = \cos(\rho) \text{ e } r_1 = \sin(\rho).$$

Siccome r_0 e r_1 sono positivi, ρ descrive solo il quadrante positivo, cioè $0 \leq \rho \leq \frac{\pi}{4}$.

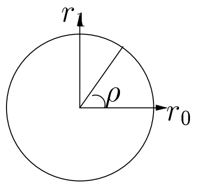

Figure 3: Il cerchio unitario di equazione $r_0^2 + r_1^2 = 1$

Ponendo $\theta = 2\rho$, otteniamo l'espressione

$$|\psi\rangle = \cos(\theta/2)e^{i\phi_0}|0\rangle + \sin(\theta/2)e^{i\phi_1}|1\rangle,$$

con $0 \leq \theta \leq \frac{\pi}{2}$, o equivalentemente

$$|\psi\rangle = e^{i\phi_0}(\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle),$$

con $\varphi = \phi_1 - \phi_0$.

Vedremo che da un punto di vista fisico il fattore $e^{i\gamma}$ si può ignorare in quanto non ha *effetti osservabili.* Di conseguenza possiamo effettivamente scrivere un qubit come

$$|\psi\rangle = \cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle,$$

che rappresenta esattamente il punto di coordinate θ e φ sulla sfera di Bloch, come mostrato Figura 1.

2 Computazione quantistica

Abbiamo studiato la descrizione quantistica degli stati di una computazione. Lo scopo di questa lezione è studiare come questi stati evolvono dando luogo ad una computazione quantistica.

Analogamente ai computer classici, un computer quantistico è formato da circuiti quantistici costituiti da *porte logiche quantistiche* elementari.

2.1 Porte logiche quantistiche a un qubit

Nel caso classico esiste un'unica porta logica (non banale) a un bit, la porta `NOT`, che implementa l'operazione logica di negazione definita mediante una tabella di verità in cui $1 \to 0$ e $0 \to 1$.

Per definire un'operazione analoga su un qubit, non possiamo limitarci a stabilire la sua azione sugli stati di base $|0\rangle$ e $|1\rangle$, ma dobbiamo specificare anche come deve essere trasformato un qubit che si trova in una sovrapposizione degli stati $|0\rangle$ e $|1\rangle$. Intuitivamente, il `NOT` dovrebbe scambiare i ruoli dei due stati fondamentali e trasformare $\alpha\,|0\rangle + \beta\,|1\rangle$ in $\beta\,|0\rangle + \alpha\,|1\rangle$. Chiaramente $|0\rangle$ si trasformerebbe in $|1\rangle$ e $|1\rangle$ in $|0\rangle$. L'operazione che implementa questo tipo di trasformazione è un'operazione *lineare* (cf. Appendice) e, come vedremo, questa è una proprietà generale della meccanica quantistica che si giustifica sperimentalmente. Un modo conveniente per rappresentare operazioni lineari è per mezzo di matrici. La matrice corrispondente al `NOT` quantistico è chiamata per motivi storici X ed è definita da:

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

Si può infatti verifcare che l'applicazione di X a un qubit $\alpha\,|0\rangle + \beta\,|1\rangle$ (scritto in notazione vettoriale) è:

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

In generale un'operazione su un singolo qubit può essere specificata da una matrice 2×2. Tuttavia non tutte le matrici 2×2 definiscono operazioni "lecite" su qubits. Ricordiamo che la condizione di normalizzazione richiede che $|\alpha^2 + \beta^2| = 1$ in qualsiasi stato quantistico $\alpha\,|0\rangle + \beta\,|1\rangle$. La stessa condizione deve valere anche per lo stato che si ottiene dopo aver effettuato l'operazione. La proprietà delle matrici che garantisce la trasformazione di un vettore unitario in un vettore che è ancora unitario si chiama *unitarietà* (cf. Appendice).

Contrariamente al caso classico in cui possiamo definire una sola operazione non banale su un singolo bit, nel caso quantistico esistono molte operazioni non banali su un singolo qubit. Oltre al `NOT` due operazioni importanti che useremo in seguito sono la porta Z e la porta di *Hadamard*:

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

che agisce solo sulla componente $|1\rangle$ scambiandone il segno,

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

Quest'ultima operazione è una delle più utili e viene usata molto spesso nella definizione di circuiti quantistici. Il suo effetto è quello di trasformare uno

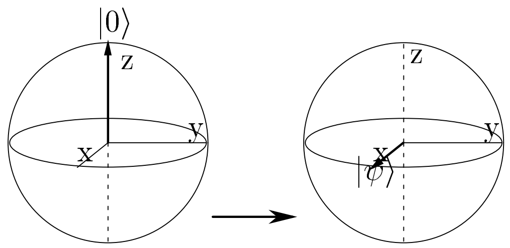

Figure 4: Visualizzazione della porta di Hadamard applicata all'input $|0\rangle$. L'output è $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

stato base in una sovrapposizione che risulta, dopo una misurazione nella base computazionale, essere 0 oppure 1 con uguale probabilità. Ad esempio, applicando H a $|0\rangle$ si ottiene:

$$H\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

cioè lo stato $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. L'effetto di H si può quindi vedere come un `NOT` eseguito a metà in modo che lo stato risultante non è ne' 0 ne' 1, bensì una sovrapposizione coerente dei due stati di base. Per questo motivo H viene spesso chiamata la "radice quadrata di `NOT`". Nota che questa espressione ha un significato solo fisico! Da un punto di vista algebrico, H^2 *non* è la matrice X. Con un semplice calcolo si può infatti verificare che H^2 è l'identità e quindi applicando due volte H ad uno stato lo lascia inalterato.

Nella sfera di Bloch l'operazione H corrisponde ad una rotazione di 90° della sfera intorno all'asse y seguita da una riflessione attraverso il piano (x, y). In Figura 4 è illustrato l'effetto dell'applicazione di H al qubit $|0\rangle$. Si può provare a visualizzare l'effetto di H sul qubit $\frac{|0\rangle+|1\rangle}{\sqrt{(2)}}$. Per effetto della rotazione e della successiva riflessione attraverso il piano x, y si otterrà nuovamente $|0\rangle$.

Le porte logiche a un qubit X, Z e H sono rappresentate graficamente come in Figura 5.

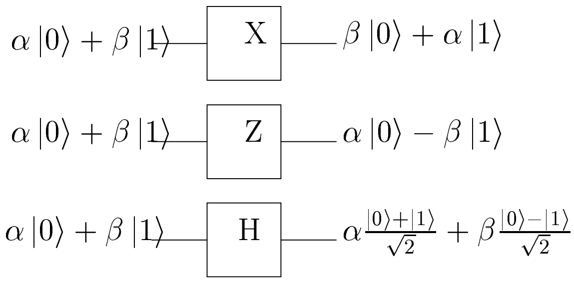

Figure 5: Le porte X, Z e H

A Richiami di Algebra Lineare

A.1 Rappresentazione di operatori lineari

Una funzione $L : \mathbb{C}^2 \mapsto \mathbb{C}^2$ si dice lineare se per ogni $a_1, a_2 \in \mathbb{C}$ e $v_1, v_2 \in \mathbb{C}^2$:

$$L(a_1 v_1 + a_2 v_2) = a_1 L(v_1) + a_2 L(v_2).$$

Dato un vettore $u \in \mathbb{C}^2$, il duale di u è la funzione lineare $L_u : \mathbb{C}^2 \mapsto \mathbb{C}$ definito da $L_u(w) = (u, w) = u^\dagger w$. Spesso si identifica L_u con $u^\dagger$. Nella notazione di Dirac il duale di un vettore $|\psi\rangle$ è denotato da $\langle\psi|$ e il prodotto scalare di $|\psi\rangle$ e $|\phi\rangle$ da $\langle\psi, \phi\rangle$. Per vettori a norma 1 il significato di $L_u(w) = \langle u, w\rangle$ è la proiezione di w nella direzione di u.

Esercizio A.1 *Dimostrare che la somma di due funzioni lineari è lineare.*

Esercizio A.2 *Dimostrare che la funzione lineare $|\psi\rangle\langle\phi| : \mathbb{C}^2 \mapsto \mathbb{C}^2$ definita da $|\psi\rangle\langle\phi|(|x\rangle) = \langle\phi, x\rangle |\psi\rangle$ è lineare.*

La rappresentazione matriciale di una funzione lineare L nella base computazionale $|0\rangle$ e $|1\rangle$ si definisce a partire da $L(|0\rangle)$ e $L(|1\rangle)$ come segue. Supponiamo che

$$L(|0\rangle) = a_{11} |0\rangle + a_{21} |1\rangle$$

e

$$L(|1\rangle) = a_{12} |0\rangle + a_{22} |1\rangle .$$

Allora possiamo scrivere L come

$$L = a_{11} |0\rangle\langle 0| + a_{21} |1\rangle\langle 0| + a_{12} |0\rangle\langle 1| + a_{22} |1\rangle\langle 1| .$$

La matrice

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

è la rappresentazione matriciale di L nella base computazionale $|0\rangle$ e $|1\rangle$.

Cambio di base

Il passaggio da una base ad un'altra è una trasformazione lineare la cui matrice si costruisce come segue. Supponiamo che i vettori $|\psi_1\rangle$ e $|\psi_2\rangle$ formino una base per $\mathbb{C}^2$ e che in tale base risulti $|0\rangle = b_{11}|\psi_1\rangle + b_{21}|\psi_2\rangle$ e $|1\rangle = b_{12}|\psi_1\rangle + b_{22}|\psi_2\rangle$. Allora la matrice del cambio di base è data da:

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Il vettore con rappresentazione $(\alpha, \beta)^T$ nella base $|0\rangle$ e $|1\rangle$, avrà coordinate $B(\alpha, \beta)^T$ rispetto alla base $|\psi_1\rangle$ e $|\psi_2\rangle$.

Esempio A.3 *Considera la base formata dai due qubits* $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ *e* $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. *La matrice del cambio di base da* $|0\rangle$, $|1\rangle$ *a* $|+\rangle$, $|-\rangle$ *è data da*

$$B = \sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Esercizio A.4 *Verificare che la rappresentazione di* L *nella nuova base è* BAB^{-1}

Esercizio A.5 *Dimostrare che la rappresentazione di* `NOT` *nella base* $|0\rangle$ *e* $|1\rangle$ *è la matrice*

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

Qual è la sua rappresentazione nella base $|+\rangle$, $|-\rangle$*?*

A.2 Matrici unitarie

Data una matrice $n \times m$ A, la trasposta A^T è definita da $(A^T)_{ij} = (A)_{ji}$. La coniugata A^* di A è la matrice $(A^*)_{ij} = (A)^*_{ij}$. La matrice aggiunta $A^\dagger$ di A è la matrice $A^\dagger = (A^T)^*$.

Una matrice A è detta unitaria se $A^\dagger = A^{-1}$, dove A^{-1} è l'inversa di A, cioè $AA^{-1} = I$ (I è la matrice identità, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$).

Teorema A.6 *Una funzione lineare trasforma un qubit in un qubit (cioè preserva vettori normalizzati) se e solo se è unitaria.*

Esercizio A.7 *Dimostrare che le matrici*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \; e \; Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

sono unitarie. X, Y *e* Z *sono dette le matrici di Pauli.*

Esercizio A.8 *Dimostrare che*

$$\langle u, Av \rangle = \left\langle A^{\dagger} u, v \right\rangle .$$

Dedurre la seguente proprietà delle matrici unitarie: M *è unitaria se e solo se preserva i prodotti scalari, cioè se e solo se* $\langle Mu, Mv \rangle = \langle u, v \rangle$*, per ogni* $u, v \in \mathbb{C}^2$.