Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

Lezione 1: Introduzione generale

1 Fisica e Computazione

La computazione è essenzialmente un processo fisico che viene eseguito su una macchina il cui funzionamento obbedisce a certe leggi fisiche. La teoria classica della computazione si basa su un modello astratto di macchina universale (la Macchina di Turing Universale) che cattura completamente il significato dell'esecuzione di un compito algoritmico su un computer. La tacita assunzione è che una macchina di Turing idealizza un dispositivo meccanico di computazione (con una memoria potenziale infinita) che obbedisce alle leggi della fisica classica.

Tuttavia le leggi della fisica sono in ultima analisi leggi meccanico- quantistiche. Queste sono le uniche in grado di giustificare i fenomeni fisici che avvengono a livello microscopico, come per esempio all'interno di un atomo. Questi fenomeni saranno imprescindibili nella costruzione di computers elettronici in un futuro ormai prossimo se la legge di Moore continuerà a valere, come ci si aspetta. Questa legge formulata già negli anni Sessanta prevedeva che la potenza di un computer sarebbe raddoppiata una volta ogni due anni. In pratica questa legge ha dimostrato fino ad oggi la sua validità, e attualmente effetti quantistici incominciano ad interferire nel funzionamento dei dispositivi elettronici man mano che le loro dimensioni diventano più piccole.

Agli inizi degli anni Ottanta, David Deutsch considerò la possibilità di formulare un modello di computazione più generale che tenesse conto delle leggi della meccanica quantistica. Questo modello noto come Computer Quantistico Universale ha portato alla concezione moderna di *computazione quantistica*.

2 Quantum bits

Il concetto fondamentale della computazione classica è il *bit*. La computazione quantistica si basa su un concetto analogo, il *quantum bit*, o in breve *qubit*, di cui descriviamo nel seguito le proprietà fondamentali sottolineandone le differenze con il bit classico.

2.1 Interpretazione matematica

Descriveremo un qubit come un oggetto matematico astratto che gode di certe particolari proprietà. La natura fisica di tale oggetto verrà chiarita successivamente osservando la corrispondenza tra le proprietà di un qubit con quelle di un qualsiasi sistema quantistico a due stati.

Lo stato di un bit classico viene descritto mediante i valori 0 e 1. Il modo piu' diretto per rappresentare lo stato di un qubit è mediante un vettore unitario in uno spazio vettoriale complesso a due dimensioni[1]. I vettori $|0\rangle$ e $|1\rangle$ formano una base ortonormale per questo spazio vettoriale, nota come *base computazionale*. La notazione '$|\rangle$' (*ket*) è detta *notazione di Dirac* dal nome del famoso fisico inglese, pioniere della teoria quantistica, che la introdusse e rappresenta la notazione standard per gli stati in meccanica quantistica. Usando la notazione classica dell'algebra lineare, possiamo rappresentare $|0\rangle$ con il vettore colonna $(1,0)^T$ e $|1\rangle$ con il vettore $(0,1)^T$, dove T indica il trasposto. Gli stati $|0\rangle$ e $|1\rangle$ di un qubit si possono vedere come i corrispondenti degli stati 0 e 1 di un bit classico. La differenza tra bits e qubits sta nel fatto che un qubit si può trovare anche in altri stati diversi da $|0\rangle$ e $|1\rangle$. Infatti, ogni combinazione lineare

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

dove α e β sono numeri complessi, è un possibile stato per un qubit. In notazione algebrica, il vettore $|\psi\rangle$ corrisponde a

$$\alpha\begin{pmatrix}1\\0\end{pmatrix}+\beta\begin{pmatrix}0\\1\end{pmatrix}\equiv\begin{pmatrix}\alpha\\\beta\end{pmatrix}$$

Tali stati sono spesso chiamati *sovrapposizioni* (superpositions).

Mentre per un bit classico possiamo sempre determinarne lo stato e stabilire con precisione se è 0 o 1, per un qubit non possiamo determinare con altrettanta precisione il suo stato quantistico, cioè i valori di α e β. La meccanica quantistica ci dice che quando misuriamo un qubit possiamo solo

[1] cf. Appendice

ottenere lo stato $|0\rangle$ con una probabilità pari a $|\alpha|^2$ oppure lo stato $|1\rangle$ con una probabilità pari a $|\beta|^2$. Per questo motivo i valori α e β sono chiamati *ampiezze di probabilità* e la somma $|\alpha|^2 + |\beta|^2$ deve essere 1. Geometricamente questo significa che gli stati di un qubit sono vettori normalizzati di lunghezza 1 (o vettori unitari).

Abbiamo quindi stabilito che un qubit si può trovare in un numero di stati che è infinitamente maggiore di quello dei possibili stati di un bit classico. Si vedrà successivamente che la realizzazione fisica di un qubit non permette di osservare direttamente questi stati: la "misurazione" di un qubit darà sempre come risultato o lo stato $|0\rangle$ oppure lo stato $|1\rangle$. Si noti tuttavia che i risultati delle misurazioni dipendono strettamente dalle proprietà specifiche dello stato su cui si sono effettuate operazioni di trasformazioni. In questo risiede essenzialmente la potenza del calcolo quantistico.

Esempio 2.1 *Un qubit si può trovare nello stato*

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,,$$

fino al momento in cui viene osservato. Nel momento in cui lo misuriamo, il risultato sarà 0 *nel 50% dei casi e* 1 *nel rimanente 50% dei casi. Cioè otterremo il risultato* 0 *con probabilità* $(1/\sqrt{2})^2 = 1/2$ *e il risultato* 1 *con probabilità* $(1/\sqrt{2})^2 = 1/2$.

2.2 Interpretazione fisica

La descrizione astratta di un qubit come un vettore in uno spazio bi- dimensionale complesso ha un corrispondente nel mondo reale. In particolare, un qualsiasi sistema fisico con almeno due livelli di energia discreti e sufficientemente separati è un candidato appropriato per rappresentare un qubit. Ad esempio possiamo considerare il sistema costituito dall'atomo di idrogeno H. In questo sistema, lo stato $|0\rangle$ del qubit può essere rappresentato dal primo livello di energia ($n = 0$), corrispondente allo stato base dell'elettrone, e lo stato $|1\rangle$ dal secondo livello di energia ($n = 1$) corrispondente allo stato eccitato dell'elettrone, come in Figura 1. Il passaggio dell'elettrone da uno stato all'altro può essere realizzato sottoponendo l'elettrone ad un impulso laser di appropriata intensità, durata e lunghezza d'onda. Riducendo opportunamente la durata, si può realizzare il passaggio di un elettrone inizialmente nello stato $|0\rangle$ ad uno stato che si trova "a metà" tra $|0\rangle$ e $|1\rangle$, corrispondente allo stato $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ dell'esempio 2.1.

Una caratteristica importante del qubit ha a che fare con la sua *misurazione*. Come illustrato nell'Esempio 2.1, quando osserviamo un qubit, il

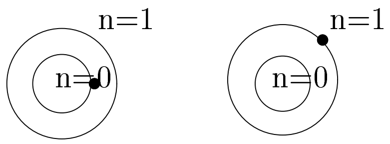

Figure 1: Qubit rappresentato da un elettrone in un atomo di idrogeno

risultato può solo essere 0 oppure 1. Inoltre, la misurazione che abbiamo fatto *cambia* lo stato del qubit facendolo collassare dalla sua sovrapposizione di $|0\rangle$ e $|1\rangle$ allo stato specifico consistente con il risultato della misurazione. Queste proprietà si spiegano mediante i principi della meccanica quantistica che illustriamo brevemente nel seguente esempio.

Un fenomeno quantistico

L'esperimento riportato nelle Figure 2 e 3 aiuta a capire il comportamento quantistico su scala atomica. Di tale comportamento non possiamo avere nessuna esperienza diretta nel mondo macroscopico.

Considera un dispositivo in grado di sparare elettroni contro una parete dove sono presenti due fori S_1 e S_2. Dietro questo schermo, un detector si sposta lungo un'altra parete con la funzione di contare gli elettroni che arrivano al suo passaggio. Si può così determinare sperimentalmente la probabilità che gli elettroni attraversino i due fori come una funzione della posizione x dell'elettrone sulla parete del detector. Si osserva che quando S_1 è chiuso, gli elettroni attraversano S_2 secondo la distribuzione $P_2(x)$, mentre se si chiude il foro S_1 tale distribuzione è $P_1(x)$. A questo punto l'esperimento procede esattamente come se invece di elettroni le particelle sparate fossero delle particelle ordinarie come ad esempio dei proiettili.

La parte interessante consiste nell'osservare quello che succede quando entrambi i fori sono aperti (Figura 3). Se si trattasse di proiettili, ci aspetteremmo di osservare una distribuzione $\frac{1}{2}(P_1(x) + P_2(x))$ dal momento che per la particella ci sono in questo caso due possibili strade ciascuna delle quali può essere presa con probabilità $P_i, i \in \{1, 2\}$. In realtà la distribuzione che si ottiene è P_{12} come raffigurata in Figura 3. P_{12} oscilla tra 0 e il valore $P_1(x)+P_2(x)$ secondo un pattern tipico dei fenomeni ondulatori (e.g. le onde dell'acqua o le radiazioni elettromagnetiche). La spiegazione sta nel fatto che quando entrambi i fori sono aperti lo stato dell'elettrone corrisponde ad una sovrapposizione di due stati corrispondenti rispettivamente alle due situazioni in cui solo il foro $S_i, i \in \{1, 2\}$ è aperto. Le associate ampiezze $\alpha_1(x)$ e

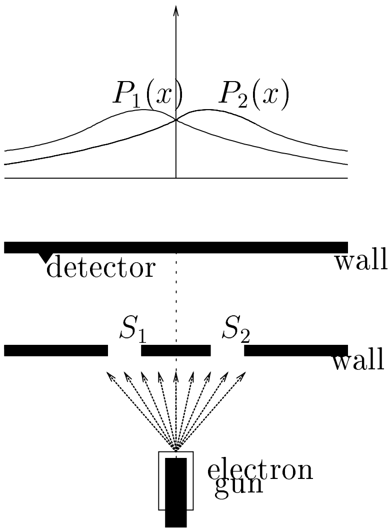

Figure 2: L'esperimento (A)

$\alpha_2(x)$ sono numeri complessi[2] da cui si ottengono le rispettive distribuzioni di probabilità $P_i(x)$. La distribuzione degli elettroni quando entrambi i fori sono aperti è data quindi da $\alpha_{12}(x) = c(\alpha_1(x) + \alpha_2(x))$, (dove c è un fattore di normalizzazione) da cui si ottiene

$$P_{12} = |\alpha_1(x) + \alpha_2(x)|^2 \approx P_1(x) + P_2(x) + 2Re(\alpha_1^*(x)\alpha_2(x)).$$

L'ultimo termine è responsabile dello strano comportamento degli elettroni. Tale comportamento è noto come *interferenza.*

Nota che l'interferenza scompare non appena tentiamo di osservare dall'esterno il comportamento dell'elettrone. In particolare, se attraverso una sorgente di luce posta tra le due pareti provassimo a osservare attraverso quale foro passa ogni elettrone, otterremmo una distribuzione di probabilità esattamente identica a quella che si otterrebbe per particelle ordinarie, cioè $\frac{1}{2}(P_1(x) + P_2(x))$.

[2]Ricordiamo che un numero complesso è della forma $z = a + ib$, dove $i = \sqrt{(}-1)$, $a = Re(z)$ è la parte reale di z, $b = Im(z)$ è la parte immaginaria di z e $a, b \in \mathbb{R}$ sono numeri reali. La *norma* o *modulo* di z è $|z| = \sqrt{a^2 + b^2}$. Il *coniugato* di z è $z^* = a - ib$. Si denota con $\mathbb{C}$ l'insieme dei numeri complessi.

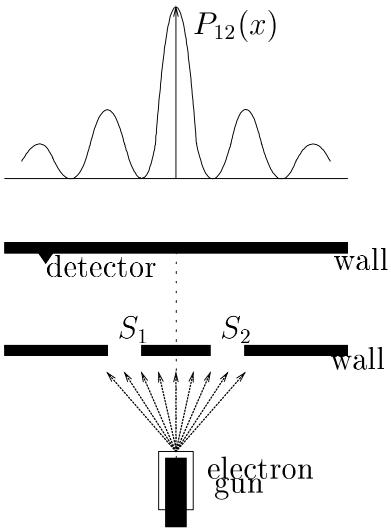

Figure 3: L'esperimento (B)

3 Registri quantistici

Con due bits classici possiamo formare quattro possibili stati: 00, 01, 10, 11. In generale, con n bits è possibile costruire 2^n stati distinti. Quanti stati si possono ottenere con n qubits? Lo spazio degli stati generato da un sistema di n qubits ha dimensione 2^n: ogni vettore normalizzato in questo spazio rappresenta un possibile stato computazionale, che chiameremo *registro quantistico a n qubits*. Questa crescita esponenziale nel numero dei qubits delle dimensioni dello spazio degli stati suggerisce la potenziale capacità di un computer quantistico di elaborare informazioni ad una velocità esponenzialmente superiore a quella di un computer classico. Si noti che per $n = 200$ si ottiene un numero che è più grande del numero di atomi nell'universo.

Formalmente un registro quantistico di n qubits è un elemento dello spazio di Hilbert 2^n-dimensionale, $\mathbb{C}^{2^n}$ (cf. Appendice), con base computazionale formata da 2^n registri a n qubits

$$|i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle$$

con $i_j \in \{0,1\}$, $1 \leq j \leq n$. Per convenienza, questo vettore della base si scrive $|i_1\rangle\,|i_2\rangle \ldots |i_n\rangle$ oppure semplicemente $|i_1 i_2 \ldots i_n\rangle$.

Consideriamo il caso di due qubits. In analogia con il singolo qubit, possiamo costruire la base computazionale dello spazio degli stati come formata dai vettori $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Come osservato precedentemente, $|x, y\rangle$ è un'abbreviazione di $|x\rangle \otimes |y\rangle$, il prodotto tensore di x e y (cf. Appendice). In notazione algebrica questi vettori corrispondono quindi a

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Un registro quantistico a due qubits è una sovrapposizione della forma:

$$|\psi\rangle = \alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle,$$

con la condizione di normalizzazione $\sum_{i \in \{0,1\}^2} |\alpha_i|^2 = 1$.

Analogamente al caso di un singolo qubit, il risultato di una misurazione sarà uno degli stati $i \in \{0,1\}^2$ con probabilità $|\alpha_i|^2$.

In un sistema di n qubits possiamo anche misurare solo un sottoinsieme degli n qubits. Per esempio, nel caso di un registro a due qubit possiamo misurare il primo qubit ottenendo come risultato 0 con probabilità $|\alpha_{00}|^2 + |\alpha_{01}|^2$. Dopo aver effettuato la misurazione lo stato collasserà a

$$\frac{\alpha_{00} |00\rangle + \alpha_{01} |01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}.$$

Nota che lo stato viene rinormalizzato per avere lunghezza 1.

Esercizio 3.1 *Scrivere le basi computazionali per un registro quantistico a 3 qubits e a 4 qubits.*

Una proprietà importante dei registri quantistici a n qubits è che non è sempre possibile decomporli negli stati dei qubit componenti. Gli stati di questo tipo sono detti *entangled*.

Esempio 3.2 (Entanglement) *Lo stato $|00\rangle + |11\rangle$ non può essere fattorizzato nel prodotto tensore di due qubits indipendenti, cioè non esistono a_1, a_2, b_1, b_2 tali che*

$$|00\rangle + |11\rangle = (a_1 |0\rangle + b_1 |1\rangle) \otimes (a_2 |0\rangle + b_2 |1\rangle).$$

Esercizio 3.3 *Dimostrare l'affermazione dell'Esempio 3.2.*

A Richiami di Algebra Lineare

A.1 Spazi vettoriali

Lo spazio vettoriale reale a due dimensioni $\mathbb{R}^2$ è l'insieme dei vettori colonna della forma

$$v = \begin{pmatrix} a \\ b \end{pmatrix}$$

dove $a, b \in \mathbb{R}$ sono numeri reali. La norma di v è data da $\|v\| = \sqrt{a^2 + b^2}$. La trasposta di v è il vettore riga $v^T = (a, b)$. Il prodotto scalare di due vettori

$$v_1 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \text{ e } v_2 = \begin{pmatrix} a_2 \\ b_2 \end{pmatrix}$$

è dato da $v_1 \cdot v_2 \stackrel{\text{def}}{=} v_1^T v_2 = (a_1, b_1) \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = a_1 a_2 + b_1 b_2 = \|v_1\| \|v_2\| \cos\theta$, dove θ è l'angolo tra v_1 e v_2. Se $v_1 \cdot v_2 = 0$, allora i due vettori sono detti ortogonali.

I vettori $\{v_i \in \mathbb{R}^2 \mid i = 1, 2, \ldots, k\}$ sono detti linearmente indipendenti se

$$a_1 v_1 + a_2 v_2 + \ldots + a_k v_k = 0, \;\; a_i \in \mathbb{R},$$

implica che $a_i = 0$ per ogni $i = 1, 2, \ldots, k$. Altrimenti sono detti linearmente dipendenti.

Una base di $\mathbb{R}^2$ è un qualsiasi insieme di vettori linearmente indipendenti tali che ogni altro vettore in $\mathbb{R}^2$ si può esprimere come combinazione lineare dei vettori nell'insieme. Ogni coppia di vettori v_1 e v_2 linearmente indipendenti forma una base per $\mathbb{R}^2$. Si dice che v_1 e v_2 formano una base ortonormale per $\mathbb{R}^2$ se $\|v_1\| = \|v_2\| = 1$ e $v_1 \cdot v_2 = 0$. I due vettori

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \; \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

formano una base ortonormale per $\mathbb{R}^2$ detta la base standard di $\mathbb{R}^2$.

Esercizio A.1 *Estendere le definizioni e proprietà date per $\mathbb{R}^2$ a $\mathbb{R}^d, d \in \mathbb{N}$.*

Analogamente, lo spazio vettoriale complesso a due dimensioni $\mathbb{C}^2$ è l'insieme dei vettori colonna della forma

$$w = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

con $\alpha, \beta \in \mathbb{C}$. La norma di w è data da $\|w\| = \sqrt{|\alpha|^2 + |\beta|^2}$, dove $|z|$ è il modulo del numero complesso z. Il coniugato complesso di w è il vettore riga $w^\dagger = (\alpha^*, \beta^*)$. In anlogia con il prodotto scalare di due vettori reali , si definisce il prodotto scalare (o inner product) di due vettori complessi

$$w_1 = \begin{pmatrix} \alpha_1 \\ \beta_1 \end{pmatrix} \; w_2 = \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix}$$

come

$$(w_1, w_2) \stackrel{\text{def}}{=} w_1^\dagger w_2 = (\alpha_1^*, \beta_1^*) \begin{pmatrix} \alpha_2 \\ \beta_2 \end{pmatrix} = \alpha_1^* \alpha_2 + \beta_1^* \beta_2.$$

Lo spazio vettoriale $\mathbb{C}^2$ con il suo prodotto scalare è detto spazio di Hilbert a due dimensioni.

Le definizioni di indipendenza lineare, base e base ortonormale sono analoghe a quelle per $\mathbb{R}^2$. I due vettori

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

formano una base ortonormale per $\mathbb{C}^2$.

A.2 Prodotto tensore

Il prodotto tensore è un'operazione che combina spazi vettoriali per formare spazi vettoriali più grandi. La costruzione generale per spazi vettoriali complessi di dimensione finita è definita come segue.

Nota che per ogni intero positivo m, lo spazio vettoriale complesso m-dimensionale $\mathbb{C}^m$ ha come base standard

$$b_1^m, b_2^m, \ldots, b_m^m,$$

dove il vettore colonna di dimensione m, b_j^m, ha componenti tutte nulle tranne la j-sima che è 1. Quindi, ogni vettore $u \in \mathbb{C}^m$ si può scrivere come $\sum_{j=1}^m u_j b_j^m$, per qualche $u_j \in \mathbb{C}$:

$$u = \begin{pmatrix} u_1 \\ \vdots \\ u_j \\ \vdots \\ u_m \end{pmatrix}$$

Dati due spazi vettoriali $\mathbb{C}^k$ e $\mathbb{C}^l$, si definisce il prodotto tensore come la funzione

$$\otimes : \mathbb{C}^k \times \mathbb{C}^l \rightarrow \mathbb{C}^{kl},$$

con

$$v \otimes w = \begin{pmatrix} v_1 w \\ \vdots \\ v_j w \\ \vdots \\ v_k w \end{pmatrix}$$

dove per ogni $1 \leq j \leq k$, $v_j w$ è la moltiplicazione del vettore colonna $w \in \mathbb{C}^l$ per lo scalare $v_j \in \mathbb{C}^l$.

Per definizione, il prodotto tensore soddisfa le seguenti proprietà. Indichiamo con z un arbitrario scalare in $\mathbb{C}$ e con V e W due generici spazi di Hilbert di dimensione k e l rispettivamente.

1. Per ogni $|v\rangle \in V$ e $|w\rangle \in W$,

$$z(|v\rangle \otimes |w\rangle) = (z\,|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z\,|w\rangle).$$

2. Per ogni $|v_1\rangle, |v_2\rangle \in V$ e $|w\rangle \in W$,

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle.$$

3. Per ogni $|v\rangle \in V$ e $|w_1\rangle, |w_2\rangle \in W$,

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle.$$

Esercizio A.2 *Dimostra la proprietà di bilinearità:*

$$\begin{aligned}&(\alpha v + \alpha' v') \otimes (\beta w + \beta' w') = \\ &\alpha\beta v \otimes w + \alpha\beta' v \otimes w' + \alpha'\beta v' \otimes w + \alpha'\beta' v' \otimes w',\end{aligned}$$

dove $\alpha, \beta, \alpha', \beta' \in \mathbb{C}$, $v, v' \in \mathbb{C}^k$ *e* $w, w' \in \mathbb{C}^l$.

Esercizio A.3 *Dimostra che:*

$$b_i^k \otimes b_j^l = b_{(i-1)l+j}^{kl}.$$

Esercizio A.4 *Dimostra che per ogni* $v, v' \in \mathbb{C}^k$ *e* $w, w' \in \mathbb{C}^l$,

$$\left\langle v \otimes w, v' \otimes w' | v \otimes w, v' \otimes w' \right\rangle = \left\langle v, v' | v, v' \right\rangle \left\langle w, w' | w, w' \right\rangle.$$