Obiettivi del corso :

Introdurre le idee e i risultati principali del quantum computing e sviluppare il background in informatica, fisica e matematica necessario per capire questi risultati.

Prerequisiti : nessuno.

Libro di testo :

Quantum Computation and Quantum Information, Michael Nielsen e Isaac Chuang, Cambridge University Press, 2000.

Introduzione generale

Un po' di storia

- Crisi della *fisica classica* e avvento della *meccanica quantistica.*
- Macchina di Turing come modello astratto di computazione (1935).

Legge di Moore (1965) e nascita della teoria di quantum computing.

Nascita e sviluppo

- R. Feynman (1982) ipotizza un modello di computazione non basato sulla fisica classica.
- Inizio anni 90: Deutsch, Bennet, Vazirani, Lloyd, Steane iniziano la ricerca di uno schema formale di computazione innovativo.

Informazione classica codificata in sequenze di bits.

Informazione quantistica immagazzinata in stati quantistici: **qubit**s.

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*.

- Interpretazione matematica
- Interpretazione fisica

Qubit come oggetto matematico

Vettore unitario nello spazio vettoriale complesso a due dimensioni $\mathbb{C}^2$:

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

$\alpha, \beta \in \mathbb{C}$.

I vettori $|0\rangle$ e $|1\rangle$ formano la *base computazionale*. Si possono vedere come i corrispondenti degli stati 0 e 1.

$|\psi\rangle$ è una *sovrapposizione* (superposition) di stati.

Algebra Lineare

Notazione di Dirac: $|\cdot\rangle$ o *ket*.

Useremo anche la notazione duale $\langle\cdot|$ o *bra* e espressioni come $\langle 0, 0\rangle$ e $\langle 1, 0\rangle$ chiamate *brakets*.

In algebra lineare:

$$|0\rangle \to \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle \to \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|\psi\rangle \to \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Qubit come oggetto fisico

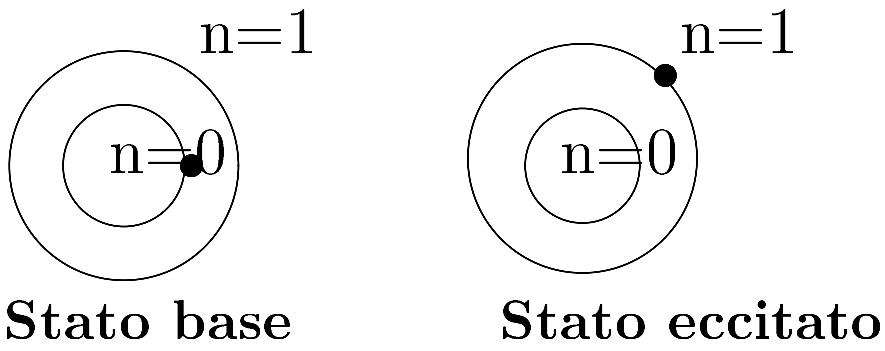

Figure 1: Qubit rappresentato da un elettrone in un atomo di idrogeno

Principio di misurazione

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

Quando viene misurato nella base computazionale, il risultato è con probabilità $(1/\sqrt{2})^2 = 1/2$ e 1 con probabilità $(1/\sqrt{2})^2 = 1/2$.

La misurazione *cambia* lo stato del qubit facendolo collassare dalla sua sovrapposizione di $\left|0\right\rangle$ e $\left|1\right\rangle$ allo stato specifico consistente con il risultato della misurazione.

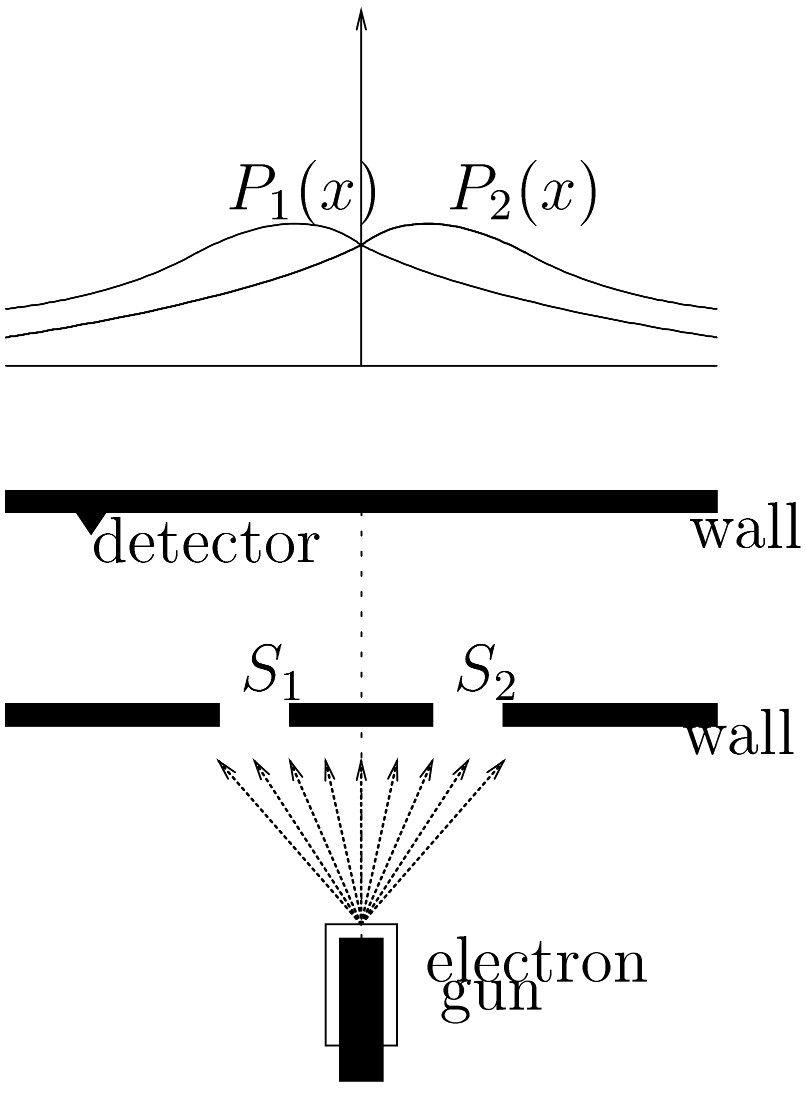

Figure 2: Un fenomeno quantistico (A)

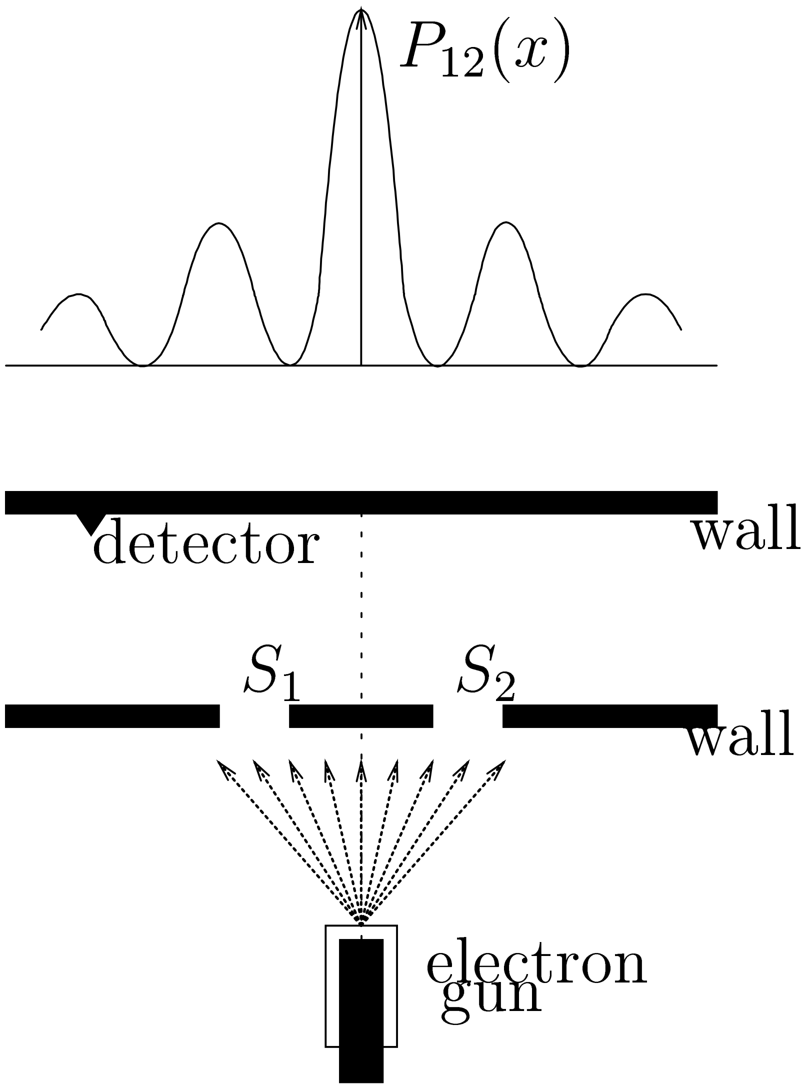

Figure 3: Un fenomeno quantistico (B)

Registri di qubits

Un sistema a due qubits ha quattro stati computazionali:

$$|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle$$

corrispondenti ai quattro possibili stati di due bits classici: 00, 01, 10, 11.

Un registro quantistico di due qubits è una sovrapposizione

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

con $\sum_{i\in\{0,1\}^2} |\alpha_i|^2 = 1$ (normalizzazione).

Quanti sono i possibili registri quantistici di n qubits?

Tutti i vettori dello spazio di Hilbert 2^n-dimensionale, $\mathbb{C}^{2^n}$!

Algebra Lineare: Prodotto tensore

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

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

con

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

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

La base computazionale di $\mathbb{C}^{kl}$ è il prodotto tensore delle basi computazionali di $\mathbb{C}^k$ e $\mathbb{C}^l$.

Base computazionale di $\mathbb{C}^4$

Lo spazio dei registri di due qubits è il prodotto tensore degli spazi dei due qubits componenti, cioè $\mathbb{C}^2 \otimes \mathbb{C}^2$.

La sua base computazionale è formata dai prodotti tensori

$$|00\rangle = |0\rangle\otimes|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \ |01\rangle = |0\rangle\otimes|1\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix},$$

$$|10\rangle = |1\rangle\otimes|0\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \ |11\rangle = |1\rangle\otimes|1\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

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

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

Si ottiene infatti:

$$a_1 a_2 |00\rangle + a_1 b_2 |01\rangle + b_1 a_2 |10\rangle + b_1 b_2 |11\rangle$$

e $a_1 b_2 = 0$ implica che o $a_1 a_2 = 0$ oppure $b_1 b_2 = 0$.

Questi stati non hanno controparte classica e sono responsabili della crescita esponenziale degli spazi di stati quantistici con il numero di qubits.