

LEZIONE 01/30

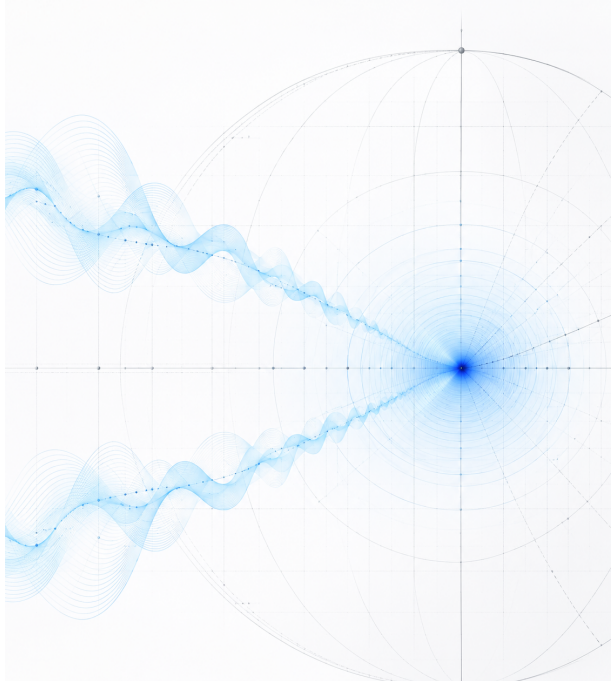
Metodi della Fisica Quantistica per l'Ingegneria

Calcolo classico e quantistico

Il computer quantistico è
soltanto un computer classico
più veloce?

Prof. Vincenzo Berardi · Politecnico di Bari

Ultimo aggiornamento: 24 Settembre 2026



I due paradigmi usano regole fisiche diverse

CALCOLO CLASSICO

bit e porte logiche

Informazione robusta, copiabile e direttamente leggibile.

CALCOLO QUANTISTICO

qubit e interferenza

Ampiezze, fasi, evoluzione unitaria e misura.

Il quantistico non sostituisce il classico: cambia il modo fisico di rappresentare e trasformare l'informazione.

Il nostro obiettivo

- 01 Distinguere** calcolabilità, efficienza e realizzazione fisica di un algoritmo
- 02 Confrontare** bit, qubit, trasformazioni, lettura, rumore e risorse
- 03 Valutare** quando un vantaggio quantistico è plausibile e quando scompare

**Domanda guida: che cosa cambia
quando il calcolo obbedisce alla fisica
quantistica?**

Ogni calcolo ha una descrizione logica e una realizzazione fisica

LIVELLO LOGICO

dati $\longrightarrow$ regole $\longrightarrow$ risultato

Specifica le operazioni, l'ordine e l'arresto.

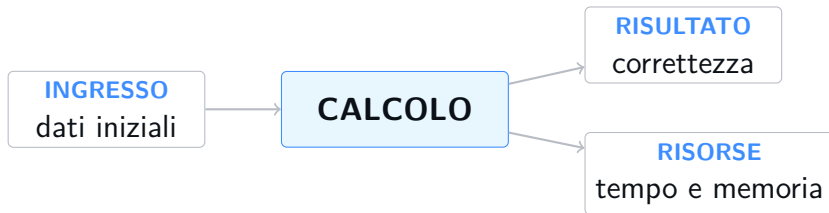
LIVELLO FISICO

materia, energia, segnali

Stabilisce quali trasformazioni sono realmente eseguibili.

Algoritmo e supporto si possono separare concettualmente, ma non sono indipendenti in assoluto.

Un algoritmo è una procedura finita che trasforma dati in risultati



La stessa funzione può essere calcolata con costi molto diversi.

La macchina universale di Turing

- 01 Formalizza** Turing isola le operazioni minime di una procedura effettiva
- 02 Simula** una macchina universale esegue la descrizione di altre macchine
- 03 Programma** istruzioni e dati diventano entrambi informazione caricabile

Ora sappiamo che il calcolo è
concettualmente possibile: ci
basta?

Calcolabilità ed efficienza sono questioni distinte

CALCOLABILITÀ

Si può calcolare?

Church e Turing hanno definito le procedure effettive.

EFFICIENZA

Con quante risorse?

Tempo, memoria, query e precisione determinano la praticabilità.

Il calcolo quantistico non amplia normalmente ciò che è calcolabile. Ma può ridurre il costo di problemi specifici.

Le risorse di calcolo necessarie possono crescere esponenzialmente

SISTEMA QUANTISTICO

n qubit

numero di ampiezze = 2^n

RISORSE

CRESCITA

$n \longrightarrow n + 1$ raddoppia lo spazio

CONSEGUENZA

simulabile $\neq$ simulabile
efficientemente

Il computer classico funziona per comparti

SOFTWARE → LOGICA

linguaggi → algoritmi → porte

Il programma diventa logica booleana.

NAND, da sola, forma un insieme universale di porte classiche.

ARCHITETTURA → FISICA

programma e dati in memoria

memoria → controllo → ALU

Registri, transistor e segnali realizzano l'architettura a programma memorizzato.

Il calcolo poggia su dispositivi reali

SUCCESSO

miniaturizzazione

Transistor, integrazione e riduzione del costo per operazione.

LIMITE

effetti microscopici

Dissipazione, fluttuazioni e tunnelling diventano rilevanti.

Il limite della miniaturizzazione non implica la fine del classico: spinge verso parallelismo e acceleratori.

La robustezza del bit è un vantaggio ingegneristico decisivo

BIT CLASSICO

0 oppure 1

Intervalli macroscopici distinti, rigenerabili e copiabili.

QUBIT

stato quantistico

Controllo delicato, misura probabilistica e no-cloning.

Non tutte le porte classiche conservano l'informazione

REVERSIBILE

$$\text{NOT}(\text{NOT}(x)) = x$$

L'uscita identifica univocamente l'ingresso.

IRREVERSIBILE

$$\text{AND}(x_1, x_2) = x_1 x_2$$

Più ingressi possono dare la stessa uscita.

$$\text{AND}(0, 0) = \text{AND}(0, 1) = 0$$

Dall'uscita di una porta irreversibile non si ricostruisce l'ingresso.

Una funzione classica può essere resa reversibile

FUNZIONE

$$f : \{0, 1\}^n \longrightarrow \{0, 1\}^m$$

$$(x, y) \longmapsto (x, y \oplus f(x))$$

L'ingresso x viene conservato.

INVERSIONE

$$f(x) \oplus f(x) = 0$$

Approfondimento

Vedi le slides che spiegano come realizza la reversibilità

Management delle risorse

COMPLESSITÀ

$T(n)$ = numero di passi

POLINOMIALE

$$O(n^k)$$

Raddoppiare n produce una crescita controllabile.

ESPONENZIALE

$$O(2^n)$$

Raddoppiare n produce un'esplosione del costo.

P, BPP e BQP classificano modelli efficienti diversi

DETERMINISTICO

P

Problemi decisionali risolti efficientemente senza casualità.

$$P \subseteq BPP \subseteq BQP$$

Inclusioni note

ERRORE LIMITATO

BPP: classico; BQP: quantistico

La fisica quantistica diventa un modello di calcolo

- 01 Simulare** Benioff e Feynman collegano computazione e dinamica quantistica
- 02 Universalizzare** Deutsch formula un modello generale di computer quantistico
- 03 Accelerare** Shor e Grover mostrano vantaggi per problemi specifici

Il qubit introduce ampiezze complesse e misura probabilistica

STATO

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

NORMALIZZAZIONE

$$|\alpha|^2 + |\beta|^2 = 1$$

MISURA

$$p(0) = |\alpha|^2, \quad p(1) = |\beta|^2$$

α e β sono ampiezze, non probabilità.

La sovrapposizione non è una memoria con due valori leggibili

INTERPRETAZIONE ERRATA

0 e 1 disponibili

Come due celle classiche leggibili contemporaneamente.

INTERPRETAZIONE CORRETTA

un solo stato coerente

Le ampiezze evolvono e interferiscono prima della misura.

La misura restituisce un solo esito; il vantaggio nasce dalla trasformazione coerente delle ampiezze.

Il vantaggio quantistico è selettivo, non universale

CORRISPONDENZA FISICA

simulazione quantistica

Il dispositivo rappresenta naturalmente stati e dinamiche quantistiche.

STRUTTURA ALGORITMICA

periodi, fasi, ricerca

Interferenza e trasformate estraggono proprietà globali mirate.

Un problema beneficia del quantistico solo quando la sua struttura coincide con le risorse del modello.

Shor e Grover due algoritmi di accelerazione quantistica

SHOR

periodicità

Fattorizzazione e logaritmo discreto; implicazioni per la crittografia a chiave pubblica; vantaggio atteso superpolinomiale.

GROVER

$$O(N) \longrightarrow O(\sqrt{N})$$

Accelerazione quadratica nel numero di query all'oracle.

Né Shor né Grover rendono efficienti tutti i problemi difficili.

Un vantaggio reale richiede tre verifiche

- 01 Problema** confrontare con approssimazione, randomizzazione, parallelismo, tensor network e acceleratori specializzati
- 02 Accesso** contabilizzare preparazione dei dati, oracle e precisione
- 03 Sistema** includere misura, ripetizioni, rumore e correzione degli errori

Chiedersi sempre: vantaggio per quale problema e con quali costi?

Input e output possono cancellare un vantaggio teorico

INGRESSO

preparare lo stato

Caricare una grande base di dati classica può dominare il costo.

USCITA

misurare pochi valori

Non si estraggono gratuitamente tutte le 2^n ampiezze.

Conta il costo end-to-end, non soltanto il nucleo quantistico dell'algoritmo.

Il rumore richiede protezione, ma la protezione ha un costo

FRAGILITÀ

decoerenza ed errori

Fase, rilassamento, porte e letture degradano il calcolo.

TOLLERANZA AI GUASTI

qubit logici

Codici quantistici e sindromi introducono un forte overhead.

La correzione rende possibile il calcolo, ma aumenta drasticamente le risorse fisiche.

Lettura e copia seguono sono diverse nel classico e nel quantistico

CLASSICO

bit copiabile e leggibile

Porte spesso irreversibili; stati intermedi accessibili.

QUANTISTICO

misura e no-cloning

Trasformazioni unitarie reversibili; la lettura modifica lo stato.

Le regole quantistiche aprono nuove possibilità, ma impongono nuovi vincoli.

Classico e quantistico hanno vantaggi complementari

PUNTI DI FORZA CLASSICI

robustezza e maturità

Memoria, controllo, costo, software e affidabilità.

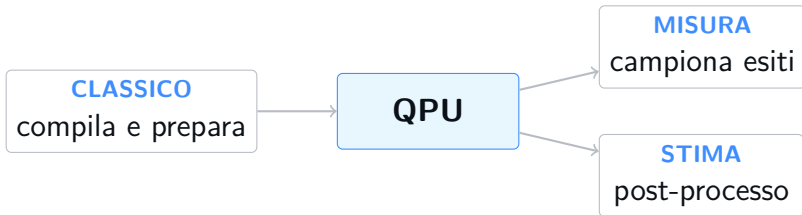
PUNTI DI FORZA QUANTISTICI

fase e interferenza

Simulazione, periodicità, ricerca e protocolli informativi.

Il confronto corretto è su un compito definito e riguarda tutte le risorse richieste.

L'architettura realistica è una cooperazione fra CPU e QPU



Il processore quantistico opera come acceleratore specializzato dentro un sistema classico.

Riassumendo

- 01 Continuità** il modello quantistico include la computazione classica
- 02 Differenza** qubit, entanglement, interferenza sono i nuovi strumenti
- 03 Criterio** il vantaggio va dimostrato problema per problema

**Prossima lezione: vettori
complessi e matrici**