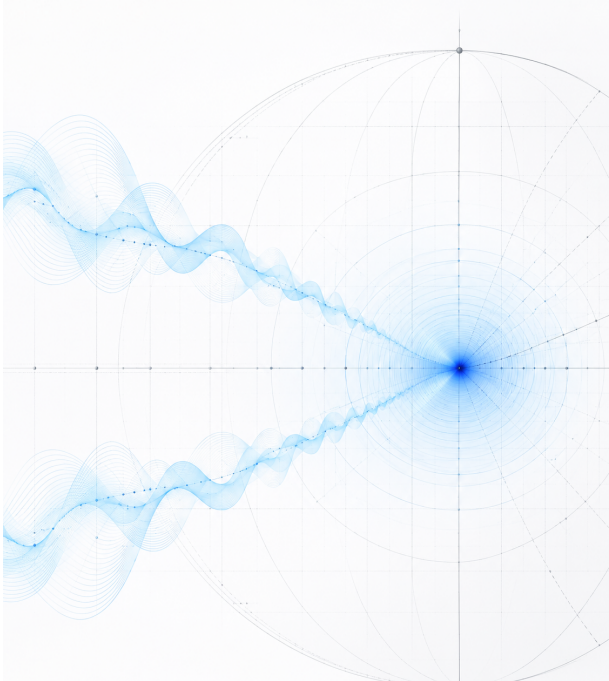
LEZIONE 15

Oracle e interferenza quantistica

Estrarre l'informazione dalle ampiezze quantistiche

Metodi della Fisica Quantistica per l'Ingegneria

Prof. Vincenzo Berardi · Politecnico di Bari



L'oracle quantistico

Una funzione $f : \{0,1\}^n \to \{0,1\}^m$ associa a ogni ingresso x il valore $f(x)$. Un **oracle** permette di valutare f senza specificare come sia realizzata.
Per rappresentarlo con un'operazione unitaria, introduciamo un registro bersaglio y:

$$\boxed{U_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle}.$$

Il primo registro non cambia; $\oplus$ è lo XOR bit a bit.
Esempio: $f(0) = 0$, $f(1) = 1$. Partiamo con il bersaglio $|0\rangle$:

$$U_f \left|0\right\rangle \left|0\right\rangle = \left|0\right\rangle \left|0 \oplus 0\right\rangle = \left|0\right\rangle \left|0\right\rangle,$$

$$U_f \left|1\right\rangle \left|0\right\rangle = \left|1\right\rangle \left|0 \oplus 1\right\rangle = \left|1\right\rangle \left|1\right\rangle.$$

Il secondo qubit contiene $f(x)$; il primo conserva x.

L'oracle è unitario

Applichiamo due volte l'oracle:

$$\begin{aligned} U_f^2 \left|x\right\rangle \left|y\right\rangle &= U_f \left|x\right\rangle \left|y \oplus f(x)\right\rangle \\ &= \left|x\right\rangle \left|y \oplus f(x) \oplus f(x)\right\rangle \\ &= \left|x\right\rangle \left|y\right\rangle . \end{aligned}$$

Poiché $f(x) \oplus f(x) = 0$, l'oracle è reversibile:

$$\boxed{U_f^2 = I, \qquad U_f^{-1} = U_f.}$$

L'operazione è anche unitaria: a ogni stato della base computazionale corrisponde uno stato distinto della stessa base.
Applicando due volte l'oracle, **il secondo registro torna al valore iniziale**, mentre il primo rimane invariato.

La funzione AND

Consideriamo la funzione classica AND di due bit:

$$f(x_1, x_0) = x_1 x_0, \qquad U_f \left|x_1 x_0\right\rangle \left|y\right\rangle = \left|x_1 x_0\right\rangle \left|y \oplus x_1 x_0\right\rangle .$$

Per il registro bersaglio inizialmente in $|0\rangle$:

$$\begin{aligned} |00\rangle|0\rangle &\mapsto |00\rangle|0\rangle & |01\rangle|0\rangle &\mapsto |01\rangle|0\rangle \\ |10\rangle|0\rangle &\mapsto |10\rangle|0\rangle & |11\rangle|0\rangle &\mapsto |11\rangle|1\rangle \end{aligned}$$

L'ingresso resta disponibile. Applicando una seconda volta U_f:

$$U_f \left|11\right\rangle \left|1\right\rangle = \left|11\right\rangle \left|1 \oplus 1\right\rangle = \left|11\right\rangle \left|0\right\rangle .$$

Abbiamo recuperato lo stato iniziale senza cancellare informazione.

Il registro ausiliario

Durante un calcolo può essere necessario **conservare temporaneamente** un risultato per utilizzarlo in un'operazione successiva.
A questo scopo si usa un registro ausiliario, detto *ancilla*. Supponiamo che inizialmente sia nello stato $|0\rangle$:

$$\boxed{|x\rangle\,|0\rangle \xrightarrow{U_f} |x\rangle\,|f(x)\rangle\,.}$$

L'ancilla contiene ora il risultato $f(x)$, mentre l'ingresso x non è cambiato.
Dopo aver utilizzato questo risultato, vogliamo riportare l'ancilla allo stato $|0\rangle$, **senza cancellare l'informazione in modo irreversibile**.
Possiamo farlo applicando nuovamente U_f; vediamo come.

Uncomputation

Consideriamo $f(x) = x$ e tre qubit: ingresso, ancilla e bersaglio. Partiamo da $|1\rangle\,|0\rangle\,|0\rangle$.

1. **Calcoliamo $f(1)$ nell'ancilla:**

$$|1\rangle\,|0\rangle\,|0\rangle \;\longrightarrow\; |1\rangle\,|1\rangle\,|0\rangle\,.$$

2. **Usiamo l'ancilla per scrivere il risultato nel bersaglio** (XOR):

$$|1\rangle\,|1\rangle\,|0\rangle \;\longrightarrow\; |1\rangle\,|1\rangle\,|1\rangle\,.$$

3. **Applichiamo di nuovo l'oracle ai primi due qubit:**

$$|1\rangle\,|1\rangle\,|1\rangle \;\longrightarrow\; \boxed{|1\rangle\,|0\rangle\,|1\rangle}.$$

L'ancilla è tornata a $|0\rangle$; il bersaglio conserva il risultato. Questo recupero del registro ausiliario si chiama *uncomputation*.

L'oracle e la fase quantistica

Consideriamo una funzione che restituisce un bit, $f(x) \in \{0, 1\}$, e prepariamo il bersaglio nello stato

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Se $f(x) = 0$, il bersaglio non cambia:

$$U_f |x\rangle |-\rangle = |x\rangle |-\rangle .$$

Se $f(x) = 1$, l'oracle scambia $|0\rangle$ e $|1\rangle$:

$$U_f |x\rangle |-\rangle = |x\rangle \frac{|1\rangle - |0\rangle}{\sqrt{2}} = - |x\rangle |-\rangle .$$

I due casi si riassumono in

$$\boxed{U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle .}$$

Il valore di $f(x)$ determina il segno dell'ampiezza.

La fase in sovrapposizione

Riprendiamo $f(0) = 0$, $f(1) = 1$. Prepariamo il primo qubit in $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e il bersaglio in $|-\rangle$.

$$\begin{aligned} U_f |+\rangle |-\rangle &= \frac{1}{\sqrt{2}} \left(U_f |0\rangle |-\rangle + U_f |1\rangle |-\rangle \right) \\ &= \frac{1}{\sqrt{2}} \left(|0\rangle |-\rangle - |1\rangle |-\rangle \right) \\ &= \boxed{|-\rangle |-\rangle}. \end{aligned}$$

Prima dell'oracle, i termini $|0\rangle$ e $|1\rangle$ avevano lo stesso segno. Dopo l'oracle hanno segni opposti.
È cambiata la fase relativa tra i due termini della sovrapposizione.

Dalla fase alla misura

Dopo l'oracle, il primo qubit è in $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Se lo misuriamo subito:

$$P(0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}, \qquad P(1) = \left|-\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}.$$

La fase relativa non cambia direttamente queste probabilità. Applichiamo allora una porta Hadamard:

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

$$= \frac{0|0\rangle + 2|1\rangle}{2} = |1\rangle .$$

$$\boxed{P(0) = 0, \qquad P(1) = 1.}$$

Le ampiezze di $|0\rangle$ si **cancellano**; quelle di $|1\rangle$ si **sommano**. Questa è l'interferenza.

Due qubit

Applichiamo una Hadamard a ciascuno dei due qubit:

$$(H \otimes H)\,|00\rangle = H\,|0\rangle \otimes H\,|0\rangle = \frac{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}{2}$$

$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

Otteniamo **quattro stati** della base computazionale, tutti con ampiezza $1/2$.

$$P(00) = P(01) = P(10) = P(11) = \frac{1}{4}.$$

Una misura restituisce uno solo dei quattro risultati possibili.

Tre qubit

Per tre qubit l'operatore è il prodotto tensoriale

$$H^{\otimes 3} = H \otimes H \otimes H, \qquad H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}.$$

$$\begin{aligned} H^{\otimes 3}|000\rangle &= H|0\rangle \otimes H|0\rangle \otimes H|0\rangle \\ &= \frac{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)}{\sqrt{8}}. \end{aligned}$$

$$\begin{aligned} H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\big(&|000\rangle + |001\rangle + |010\rangle + |011\rangle \\ &+ |100\rangle + |101\rangle + |110\rangle + |111\rangle\big). \end{aligned}$$

Otteniamo **otto stati**, tutti con ampiezza $1/\sqrt{8}$.

n qubit

Negli esempi precedenti abbiamo ottenuto quattro stati con due qubit e otto stati con tre qubit. Con n qubit, applicando una Hadamard a ciascuno:

$$H^{\otimes n}\,|0\rangle^{\otimes n} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} = \boxed{\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle}.$$

Il risultato è una sovrapposizione dei 2^n **stati** della base computazionale, tutti con la stessa ampiezza $1/\sqrt{2^n}$.

$$\boxed{2 \text{ qubit} \to 4 \text{ stati}, \quad 3 \text{ qubit} \to 8 \text{ stati}, \quad n \text{ qubit} \to 2^n \text{ stati}.}$$

Oracle e parallelismo

L'oracle agisce su un singolo ingresso secondo la regola

$$U_f \left|x\right\rangle \left|0\right\rangle = \left|x\right\rangle \left|f(x)\right\rangle .$$

Prepariamo il primo qubit nella sovrapposizione $\left|\psi\right\rangle = (\left|0\right\rangle + \left|1\right\rangle)/\sqrt{2}$ e il bersaglio in $\left|0\right\rangle$. Per la **linearità** di U_f:

$$U_f \left|\psi\right\rangle \left|0\right\rangle = \frac{U_f \left|0\right\rangle \left|0\right\rangle + U_f \left|1\right\rangle \left|0\right\rangle}{\sqrt{2}} = \frac{\left|0\right\rangle \left|f(0)\right\rangle + \left|1\right\rangle \left|f(1)\right\rangle}{\sqrt{2}}.$$

L'oracle agisce sulle **due componenti** della sovrapposizione con un'unica applicazione. Una misura, però, non legge entrambi i valori $f(0)$ e $f(1)$.

AND in sovrapposizione

I primi due qubit sono in sovrapposizione; il bersaglio parte da $|0\rangle$:

$$|\Psi_{\text{in}}\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|0\rangle\,.$$

Per $f(x_1, x_0) = x_1 x_0$, l'oracle agisce sui quattro termini:

$$|00\rangle\,|0\rangle \longrightarrow |00\rangle\,|0\rangle \qquad |01\rangle\,|0\rangle \longrightarrow |01\rangle\,|0\rangle$$
$$|10\rangle\,|0\rangle \longrightarrow |10\rangle\,|0\rangle \qquad |11\rangle\,|0\rangle \longrightarrow |11\rangle\,|1\rangle$$

Per linearità, il risultato è la sovrapposizione degli stati ottenuti:

$$\boxed{U_f\,|\Psi_{\text{in}}\rangle = \frac{1}{2}(|00\rangle\,|0\rangle + |01\rangle\,|0\rangle + |10\rangle\,|0\rangle + |11\rangle\,|1\rangle).}$$

Una misura restituisce **uno** dei quattro stati, con probabilità $1/4$.

Parallelismo su n qubit

L'esempio con la AND mostra che un oracle può agire su più ingressi presenti in sovrapposizione. Con n qubit di ingresso e un registro bersaglio inizialmente a zero:

$$|\Psi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle\,|0^m\rangle\,.$$

Per la linearità dell'oracle:

$$U_f\,|\Psi_{\text{in}}\rangle = \frac{1}{\sqrt{2^n}} \sum_x U_f\,|x\rangle\,|0^m\rangle = \boxed{\frac{1}{\sqrt{2^n}} \sum_x |x\rangle\,|f(x)\rangle}\,.$$

L'oracle agisce su tutte le componenti della sovrapposizione, ma una **misura non permette di leggere tutti i risultati**.

Il limite del parallelismo

Elaborazione classica parallela

- Più unità elaborano dati differenti.
- I risultati possono essere memorizzati e letti separatamente.

Elaborazione quantistica coerente

- Un'unitaria agisce su una sovrapposizione.
- Una misura restituisce un solo risultato.

Il parallelismo quantistico **non permette di leggere insieme** tutti i valori di una funzione. L'**interferenza** permette invece di ottenere informazioni sulla funzione attraverso le probabilità dei risultati della misura.

Phase kickback

Consideriamo una porta *controlled-U*: applica U al bersaglio solo quando il qubit di controllo è $|1\rangle$. Supponiamo che il bersaglio sia un **autostato** $|u\rangle$ di U:

$$U|u\rangle = e^{i\phi}|u\rangle .$$

L'azione di U lascia quindi invariato $|u\rangle$ e introduce una fase $e^{i\phi}$. Se il controllo è $\alpha|0\rangle + \beta|1\rangle$, per linearità:

$$\begin{aligned} C(U)(\alpha|0\rangle + \beta|1\rangle)|u\rangle &= \alpha|0\rangle|u\rangle + \beta|1\rangle U|u\rangle \\ &= \boxed{(\alpha|0\rangle + \beta e^{i\phi}|1\rangle)|u\rangle}. \end{aligned}$$

Risultato: il bersaglio conserva $|u\rangle$; il ramo $|1\rangle$ del controllo acquista la fase $e^{i\phi}$.

Fase e probabilità

Con il controllo iniziale $|+\rangle$, dopo il kickback abbiamo

$$|\chi\rangle = \frac{|0\rangle + e^{i\phi}|1\rangle}{\sqrt{2}}.$$

Applicando H:

$$H|\chi\rangle = \frac{1}{2}[(1+e^{i\phi})|0\rangle + (1-e^{i\phi})|1\rangle].$$

Le probabilità nella base computazionale sono

$$\boxed{P(0) = \frac{|1+e^{i\phi}|^2}{4} = \frac{1+\cos\phi}{2}}, \qquad \boxed{P(1) = \frac{1-\cos\phi}{2}}.$$

Adesso ϕ ha un effetto misurabile, benché una misura prima di H avrebbe dato $P(0) = P(1) = 1/2$.

Calcolo delle probabilità

Usiamo $|z|^2 = zz^*$ e $e^{i\phi} + e^{-i\phi} = 2\cos\phi$:

$$|1 + e^{i\phi}|^2 = (1 + e^{i\phi})(1 + e^{-i\phi}) = 2 + 2\cos\phi = 4\cos^2\frac{\phi}{2},$$

$$|1 - e^{i\phi}|^2 = 2 - 2\cos\phi = 4\sin^2\frac{\phi}{2}.$$

Quindi le probabilità di misura sono

$$\boxed{P(0) = \cos^2\frac{\phi}{2}, \qquad P(1) = \sin^2\frac{\phi}{2}.}$$

Esempio: $\phi = \pi/3$

Dopo il phase kickback e la Hadamard finale,

$$P(0) = \cos^2\left(\frac{\phi}{2}\right), \qquad P(1) = \sin^2\left(\frac{\phi}{2}\right).$$

Per $\phi = \pi/3$:

$$\boxed{P(0) = \cos^2\frac{\pi}{6} = \frac{3}{4}}, \qquad \boxed{P(1) = \sin^2\frac{\pi}{6} = \frac{1}{4}}.$$

La fase non è stata misurata direttamente: è stata convertita in una **distribuzione di probabilità**.

Schema guida: sovrapposizione → codifica in fase → interferenza → misura.

Lo shot

Uno *shot* è **una singola esecuzione completa** del circuito: dalla preparazione dello stato iniziale alla misura finale. **Esempio:** prepariamo un qubit in $|0\rangle$, applichiamo H e misuriamo:

$$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{\text{misura}} 0 \text{ oppure } 1.$$

$$\boxed{P(0) = \tfrac{1}{2}, \qquad P(1) = \tfrac{1}{2}.}$$

Uno shot restituisce un solo risultato, non entrambi. Per un altro shot dobbiamo **ripreparare** $|0\rangle$, applicare di nuovo H e misurare nuovamente. Ripetendo il circuito possiamo contare gli esiti e stimarne le probabilità.

Mille shot

Consideriamo lo stato normalizzato

$$|\psi\rangle = \sqrt{0.7}\,|0\rangle + e^{i\phi}\sqrt{0.3}\,|1\rangle\,.$$

Nella base computazionale:

$$P(0) = 0.7, \qquad P(1) = 0.3.$$

In $N = 1000$ esecuzioni indipendenti i **conteggi medi attesi** sono

$$\mathbb{E}[N_0] = 1000 \cdot 0.7 = 700, \qquad \mathbb{E}[N_1] = 1000 \cdot 0.3 = 300.$$

I conteggi effettivi fluttuano: 700 e 300 non sono risultati garantiti.

Tre shot: probabilità delle sequenze

Ripetiamo tre volte lo stesso circuito, **ripreparando ogni volta lo stesso stato**. Misuriamo un qubit e vogliamo contare quante volte il risultato è 1.

$$P(1) = p, \qquad P(0) = 1 - p.$$

Indichiamo con K il **numero di risultati uguali a** 1 nei tre shot. Per esempio, $K = 2$ significa che due misure danno 1 e una dà 0. **Tre sequenze possibili con** $K = 2$**:**

$$110, \qquad 101, \qquad 011.$$

Gli shot sono indipendenti: per una sequenza fissata, **moltiplichiamo** le probabilità dei tre esiti.

$$P(110) = p \cdot p \cdot (1 - p) = p^2(1 - p),$$
$$P(101) = p \cdot (1 - p) \cdot p = p^2(1 - p),$$
$$P(011) = (1 - p) \cdot p \cdot p = p^2(1 - p).$$

Dal conteggio alla distribuzione binomiale

Le sequenze 110, 101 e 011 sono **mutuamente esclusive**: in tre shot se ne può osservare una sola. Per ottenere la probabilità di $K = 2$ dobbiamo quindi **sommarle**:

$$\begin{aligned} P(K=2) &= P(110) + P(101) + P(011) \\ &= p^2(1-p) + p^2(1-p) + p^2(1-p) \\ &= \boxed{3p^2(1-p)}. \end{aligned}$$

Il fattore 3 conta i modi di collocare due risultati 1 in tre shot:

$$\binom{3}{2} = \frac{3!}{2!\,1!} = 3.$$

Per N shot indipendenti, la probabilità di osservare **esattamente** k **risultati uguali a** 1 è

$$\boxed{P(K=k) = \binom{N}{k} p^k (1-p)^{N-k}}.$$

Precisione della stima

Su N shot, se il risultato che ci interessa compare K volte, la probabilità viene stimata mediante la frequenza relativa:

$$\boxed{\hat{p} = \frac{K}{N}.}$$

Il numero K fluttua attorno alla media Np, con deviazione standard $\sigma_K = \sqrt{Np(1-p)}$. Poiché $\hat{p} = K/N$, anche la stima fluttua:

$$\boxed{\sigma_{\hat{p}} = \frac{\sigma_K}{N} = \sqrt{\frac{p(1-p)}{N}}.}$$

La precisione cresce con il numero di shot: $\sigma_{\hat{p}} \propto N^{-1/2}$. Per dimezzare l'incertezza occorrono quattro volte gli shot.

Esempio: $p = 0.3$

Calcoliamo le fluttuazioni attorno al conteggio medio di 300:

$$\sigma_K = \sqrt{1000 \cdot 0.3 \cdot 0.7} = \sqrt{210} \simeq 14.5.$$

Per la frequenza relativa,

$$\boxed{\sigma_{\hat{p}} = \sqrt{\frac{0.3 \cdot 0.7}{1000}} \simeq 0.0145.}$$

La precisione statistica tipica migliora come $1/\sqrt{N}$:

$$\sigma_{\hat{p}} \propto N^{-1/2}, \qquad \text{errore dimezzato} \implies \text{shot quadruplicati.}$$

Questa incertezza riguarda il **campionamento ideale**; eventuali errori sperimentali richiedono un'analisi separata.

Risorse del circuito

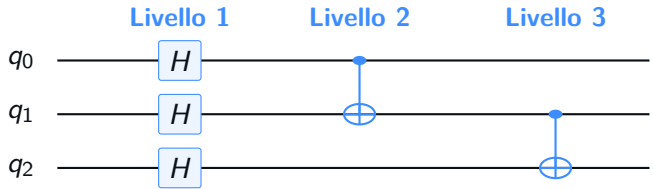
Per valutare un circuito quantistico consideriamo:

- **Numero di qubit**: qubit dei registri di ingresso (*input*) e dei registri ausiliari (*ancilla*), oltre agli altri registri utilizzati.
- **Numero di porte**: totale delle operazioni elementari.
- **Profondità (*depth*)**: numero di passaggi successivi. Le porte eseguibili contemporaneamente su qubit diversi contano come un solo passaggio.
- **Query**: numero di applicazioni dell'oracle.
- **Shot**: numero di esecuzioni complete per ottenere i risultati di misura.

Numero di porte e profondità non coincidono necessariamente.

I livelli del circuito

Un **livello** raccoglie le porte eseguibili nello stesso momento, perché agiscono su qubit diversi. Consideriamo questo circuito:



- **Livello 1**: le tre H si eseguono insieme.
- **Livello 2**: $\mathrm{CNOT}(q_0 \to q_1)$.
- **Livello 3**: $\mathrm{CNOT}(q_1 \to q_2)$, dopo la precedente: entrambe coinvolgono q_1.

Totale: 3 qubit, 5 porte e profondità 3.

Le query

Una query è una singola applicazione dell'oracle U_f. Un algoritmo può richiamare lo stesso oracle più volte. Per esempio:

	Algoritmo A	Algoritmo B
Applicazioni di U_f	3	10
Numero di query	3	10

L'algoritmo A usa meno query dell'algoritmo B. **Attenzione**: un oracle non corrisponde necessariamente a una singola porta. Per realizzare U_f possono servire numerose porte elementari. **Il numero di query conta le interrogazioni dell'oracle, non tutte le porte del circuito.**

Costo degli shot

Un circuito breve può richiedere molti shot per stimare con precisione una probabilità.

$$\sigma_{\hat{p}} = \sqrt{\frac{p(1-p)}{N}}.$$

Viceversa, un circuito ideale che genera con certezza un bit corretto può richiedere una sola esecuzione per leggere quel bit.

Costo per shot

- qubit e gate count;
- depth e oracle.

Costo della stima

- numero di ripetizioni;
- precisione e confidenza desiderate.

Calcolo classico e quantistico

Entrambi i modelli elaborano informazioni attraverso **registri e circuiti**, ma trattano diversamente gli stati e i risultati.

Calcolo classico

- I registri contengono valori di bit.
- Le operazioni modificano i valori logici.
- I risultati possono essere letti direttamente.

Calcolo quantistico

- I registri possono trovarsi in sovrapposizione.
- Le operazioni unitarie modificano le ampiezze e le fasi.
- La misura restituisce un esito classico probabilistico.

Il vantaggio quantistico non è automatico: dipende dal problema, dall'algoritmo e dalle risorse necessarie per ottenere il risultato.