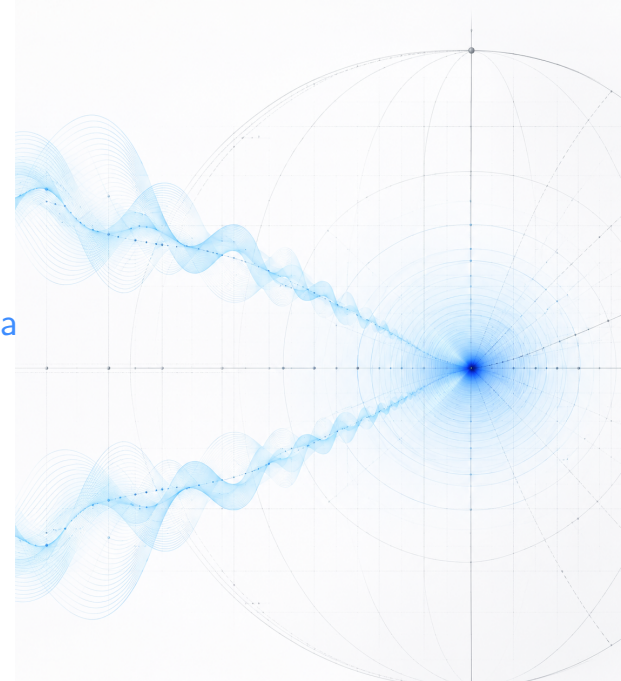
LEZIONE 18

L’algoritmo di Deutsch

Una proprietà globale con una sola query

Metodi della Fisica Quantistica per l’Ingegneria

Prof. Vincenzo Berardi · Politecnico di Bari



Dalla lezione 17 al problema di Deutsch

Nella lezione precedente abbiamo studiato i *promise problems*: si cerca una proprietà globale della funzione, non tutta la sua tabella. Ora consideriamo la più semplice funzione booleana:

$$\boxed{f : \{0,1\} \longrightarrow \{0,1\}.}$$

Il dominio contiene solo due ingressi, $x = 0$ e $x = 1$.

Obiettivo: stabilire se $f(0) = f(1)$ oppure $f(0) \neq f(1)$.

Le quattro funzioni possibili

La funzione è determinata da una coppia di valori, $(f(0), f(1))$.

Funzione	$f(0)$	$f(1)$	Classe
f_0	0	0	costante
f_1	0	1	bilanciata
f_2	1	0	bilanciata
f_3	1	1	costante

Non vogliamo sapere *quale* funzione sia stata scelta, ma *a quale classe* appartenga.

Costante oppure bilanciata

Costante: i due valori coincidono.

$$f(0) = f(1) \quad \Longleftrightarrow \quad f \in \{f_0, f_3\}.$$

Bilanciata: i due valori sono diversi.

$$f(0) \neq f(1) \quad \Longleftrightarrow \quad f \in \{f_1, f_2\}.$$

Il risultato cercato è un singolo bit:

$$f(0) \oplus f(1) = \begin{cases} 0, & \text{costante,} \\ 1, & \text{bilanciata.} \end{cases}$$

Per un ingresso di un solo bit, ogni funzione è necessariamente costante o bilanciata.

La procedura classica: prima query

Supponiamo di poter interrogare f soltanto tramite un *oracle* classico. Chiediamo $f(0)$ e otteniamo, per esempio,

$$\boxed{f(0) = 0.}$$

Dopo questa risposta sono ancora possibili

	$f(0)$	$f(1)$	classe
f_0	0	0	costante
f_1	0	1	bilanciata

Una sola interrogazione classica non è sufficiente.

La procedura classica: seconda query

Per distinguere le due possibilità è necessario conoscere anche $f(1)$.

Se $f(1) = 0$	**Se** $f(1) = 1$
$f(0) = f(1)$	$f(0) \neq f(1)$
COSTANTE	**BILANCIATA**

L'argomento non dipende dal primo risultato: se $f(0) = 1$, rimangono comunque due classi compatibili.

Il limite classico è esatto

Dopo una query, per ogni risposta osservata, rimangono possibili una funzione costante e una bilanciata. Una seconda query è sempre sufficiente: basta confrontare $f(0)$ e $f(1)$.

$$\boxed{Q_{\mathrm{C}}^{\mathrm{det,exact}} = 2.}$$

Un esempio di esecuzione classica

L'oracle implementa la funzione f_2, che non è nota a priori all'algoritmo.I suoi valori sono

$$f(0) = 1, \qquad f(1) = 0.$$

1. Prima query: $x = 0 \longrightarrow f(0) = 1$.
2. Il risultato è compatibile sia con f_2 sia con f_3.
3. Seconda query: $x = 1 \longrightarrow f(1) = 0$.

Poiché $1 \neq 0$, concludiamo che f è bilanciata.

Domanda: un oracle quantistico consente di decidere con una sola query?

L'idea dell'algoritmo quantistico

L'algoritmo di Deutsch non legge contemporaneamente $f(0)$ e $f(1)$.

1. Prepara una sovrapposizione dei due ingressi.
2. Codifica i valori della funzione nelle **fasi** delle ampiezze.
3. Fa interferire le ampiezze per rendere misurabile la proprietà globale.

L'oracle quantistico reversibile

Utilizziamo due qubit: uno di ingresso e un'*ancilla*. La trasformazione unitaria associata alla funzione booleana è

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

L'ingresso x viene conservato; il secondo qubit cambia se $f(x) = 1$. Il modello reversibile e il phase kickback sono stati introdotti nel capitolo 6.

Preparazione: perché partire da $|01\rangle$?

Il primo qubit deve esplorare coerentemente gli ingressi 0 e 1. Il secondo deve essere preparato in $|-\rangle$ per trasformare l'azione dell'oracle in una fase. Partiamo da

$$\boxed{|\psi_0\rangle = |0\rangle\,|1\rangle\,.}$$

Applichiamo una Hadamard a ciascun qubit:

$$\boxed{|\psi_1\rangle = (H \otimes H)\,|01\rangle = |+\rangle\,|-\rangle\,.}$$

$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

L'ancilla è un autostato di X

Ricordiamo che

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

Poiché $X|0\rangle = |1\rangle$ e $X|1\rangle = |0\rangle$,

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

$$\boxed{X|-\rangle = -|-\rangle.}$$

Phase kickback: la relazione essenziale

Sull'ancilla $|-\rangle$, l'oracle agisce come

$$\begin{aligned} U_f |x\rangle |-\rangle &= \frac{U_f |x\rangle |0\rangle - U_f |x\rangle |1\rangle}{\sqrt{2}} \\ &= \frac{|x\rangle |f(x)\rangle - |x\rangle |1 \oplus f(x)\rangle}{\sqrt{2}} \\ &= \boxed{(-1)^{f(x)} |x\rangle |-\rangle}. \end{aligned}$$

$$\begin{aligned} f(x) = 0 &\implies +|x\rangle |-\rangle , \\ f(x) = 1 &\implies -|x\rangle |-\rangle . \end{aligned}$$

La funzione controlla quindi il segno dell'ampiezza associata a $|x\rangle$.

Una sola query su una sovrapposizione

Lo stato di ingresso è

$$|\psi_1\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |-\rangle \,.$$

Per linearità, dopo *una* applicazione di U_f,

$$|\psi_2\rangle = U_f\,|\psi_1\rangle = \frac{U_f\,|0\rangle\,|-\rangle + U_f\,|1\rangle\,|-\rangle}{\sqrt{2}}$$
$$= \frac{(-1)^{f(0)}\,|0\rangle + (-1)^{f(1)}\,|1\rangle}{\sqrt{2}} \otimes |-\rangle \,.$$

I valori $f(0)$ e $f(1)$ determinano le fasi relative nel primo qubit.

Funzioni costanti: i due segni coincidono

Se $f(0) = f(1) = 0$, le due componenti rimangono positive:

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

Se $f(0) = f(1) = 1$, entrambe cambiano segno:

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

In entrambi i casi, a meno di una fase globale, il primo qubit è $|+\rangle$.

$$\boxed{f \text{ costante} \implies |+\rangle .}$$

Funzioni bilanciate: i segni sono opposti

Se $(f(0), f(1)) = (0, 1)$, lo stato diventa

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

Se $(f(0), f(1)) = (1, 0)$, lo stato diventa

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

A meno di una fase globale, il primo qubit è $|-\rangle$.

$$\boxed{f \text{ bilanciata} \implies |-\rangle\,.}$$

I quattro stati dopo l'oracle

Funzione	$f(0)$	$f(1)$	Primo qubit dopo U_f
f_0	0	0	$\lvert+\rangle$
f_1	0	1	$\lvert-\rangle$
f_2	1	0	$-\lvert-\rangle$
f_3	1	1	$-\lvert+\rangle$

Il segno complessivo -1 è una fase globale: non modifica le probabilità.

Perché non misurare subito?

Il primo qubit è $|+\rangle$ oppure $|-\rangle$, a meno di una fase globale. Ma una misura nella base computazionale dà, in entrambi i casi,

$$|\langle 0|+\rangle|^2 = |\langle 1|+\rangle|^2 = \tfrac{1}{2},$$
$$|\langle 0|-\rangle|^2 = |\langle 1|-\rangle|^2 = \tfrac{1}{2}.$$

La distinzione è nelle fasi, non nelle probabilità della misura diretta.

L'ultima Hadamard cambia la base di lettura

La porta H trasforma gli stati della base $\{|+\rangle, |-\rangle\}$ in quelli della base computazionale:

$$\boxed{H|+\rangle = |0\rangle, \qquad H|-\rangle = |1\rangle.}$$

Pertanto,

$$f \text{ costante} \implies \pm|+\rangle \xrightarrow{H} \pm|0\rangle,$$
$$f \text{ bilanciata} \implies \pm|-\rangle \xrightarrow{H} \pm|1\rangle.$$

La seconda Hadamard rende osservabile la distinzione prodotta dal phase kickback.

Interferenza: il calcolo algebrico

Poniamo $a = (-1)^{f(0)}$ e $b = (-1)^{f(1)}$. Il primo qubit dopo l'oracle è $(a\,|0\rangle + b\,|1\rangle)/\sqrt{2}$.

Applicando H e raccogliendo i termini,

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

$$= \boxed{\frac{(a+b)\,|0\rangle + (a-b)\,|1\rangle}{2}}.$$

Le ampiezze si sommano oppure si cancellano a seconda della classe di f.

Stato completo dopo la seconda Hadamard

Rimettendo $a = (-1)^{f(0)}$ e $b = (-1)^{f(1)}$,

$$|\psi_3\rangle = \frac{1}{2}\Big[\big((-1)^{f(0)} + (-1)^{f(1)}\big)\,|0\rangle + \big((-1)^{f(0)} - (-1)^{f(1)}\big)\,|1\rangle\Big] \otimes |-\rangle\,.$$

Per f costante, il coefficiente di $|1\rangle$ è nullo; per f bilanciata, quello di $|0\rangle$ è nullo.

$$|\psi_3\rangle = \begin{cases} \pm\,|0\rangle\,|-\rangle\,, & f \text{ costante,} \\ \pm\,|1\rangle\,|-\rangle\,, & f \text{ bilanciata.} \end{cases}$$

La misura fornisce la risposta esatta

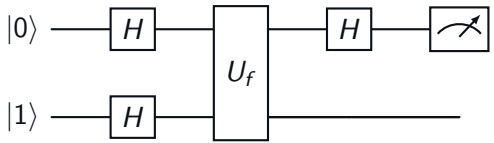
Misuriamo **soltanto il primo qubit** nella base $\{|0\rangle, |1\rangle\}$.

Risultato 0	**Risultato** 1
COSTANTE	BILANCIATA

La probabilità di ottenere la risposta corretta è

$$\boxed{P_{\text{successo}} = 1 \qquad \text{(modello ideale).}}$$

Circuito completo dell'algoritmo di Deutsch



1. Le due Hadamard iniziali preparano $|+\rangle\,|-\rangle$.
2. La *singola query* a U_f introduce i segni $(-1)^{f(x)}$.
3. L'ultima Hadamard converte la fase relativa nel bit misurato.

Nel circuito compare una sola chiamata a U_f.

Esempio 1: funzione costante $f(x) = 0$

Per $f(0) = f(1) = 0$, l'oracle non cambia i segni delle ampiezze.

$$
\begin{aligned}
|\psi_1\rangle &= |+\rangle\,|-\rangle\,, \\
|\psi_2\rangle &= |+\rangle\,|-\rangle\,, \\
|\psi_3\rangle &= (H\,|+\rangle)\,|-\rangle = |0\rangle\,|-\rangle\,.
\end{aligned}
$$

La misura produce 0 con probabilità uno: **funzione costante**.

Esempio 2: funzione costante $f(x) = 1$

Per $f(0) = f(1) = 1$, entrambe le componenti acquisiscono lo stesso segno.

$$
\begin{aligned}
|\psi_1\rangle &= |+\rangle\,|-\rangle\,, \\
|\psi_2\rangle &= -\,|+\rangle\,|-\rangle\,, \\
|\psi_3\rangle &= -\,|0\rangle\,|-\rangle\,.
\end{aligned}
$$

Il segno complessivo -1 non cambia le probabilità di misura. Anche in questo caso la misura restituisce 0: **funzione costante**.

Esempio 3: funzione bilanciata $f(x) = x$

Per $f(0) = 0$ e $f(1) = 1$,

$$
\begin{aligned}
|\psi_1\rangle &= |+\rangle\,|-\rangle\,, \\
|\psi_2\rangle &= \frac{|0\rangle - |1\rangle}{\sqrt{2}}\,|-\rangle = |-\rangle\,|-\rangle\,, \\
|\psi_3\rangle &= (H\,|-\rangle)\,|-\rangle = |1\rangle\,|-\rangle\,.
\end{aligned}
$$

La misura produce 1 con probabilità uno: **funzione bilanciata**.

Esempio 4: funzione bilanciata $f(x) = 1 \oplus x$

Per $f(0) = 1$ e $f(1) = 0$,

$$
\begin{aligned}
|\psi_1\rangle &= |+\rangle\,|-\rangle\,, \\
|\psi_2\rangle &= \frac{-\,|0\rangle + |1\rangle}{\sqrt{2}}\,|-\rangle = -\,|-\rangle\,|-\rangle\,, \\
|\psi_3\rangle &= -(H\,|-\rangle)\,|-\rangle = -\,|1\rangle\,|-\rangle\,.
\end{aligned}
$$

La misura produce ancora 1: **funzione bilanciata**. Il secondo caso bilanciato differisce dal primo soltanto per una fase globale.

Confronto dei costi: due query contro una

Metodo	Query	Successo
Classico deterministico, esatto	2	1
Quantistico (Deutsch), ideale	1	1

Attenzione: il vantaggio riguarda il *numero di interrogazioni*, non il tempo totale di esecuzione o il costo di costruzione dell'oracle.

Deutsch è soprattutto un esempio fondativo di vantaggio nel modello a oracle.

Che cosa viene letto davvero?

Dopo U_f, il primo qubit contiene informazioni sui valori di f **nelle fasi**. Non possiamo ricavare entrambe le risposte $f(0)$ e $f(1)$ tramite una sola misura. La Hadamard finale fa interferire le ampiezze e rende misurabile direttamente

$$\boxed{f(0) \oplus f(1).}$$

L'informazione estratta è una proprietà globale della funzione, non la sua tabella.

Possibile applicazione: un dispositivo a due modalità

Consideriamo un dispositivo che può operare nelle modalità $x = 0$ e $x = 1$. Definiamo

$$f(x) = \begin{cases} 1, & \text{se il dispositivo segnala un'anomalia,} \\ 0, & \text{altrimenti.} \end{cases}$$

La domanda è se la segnalazione cambi fra le due modalità:

$$\boxed{f(0) \oplus f(1) = 0 \iff \text{segnalazione identica.}}$$

Una query quantistica ideale distingue i due casi tramite l'interferenza.

La struttura dell'algoritmo di Deutsch



$$\boxed{\text{risultato misurato} = f(0) \oplus f(1).}$$

Nella prossima lezione: il problema di Deutsch–Jozsa con n bit di ingresso.