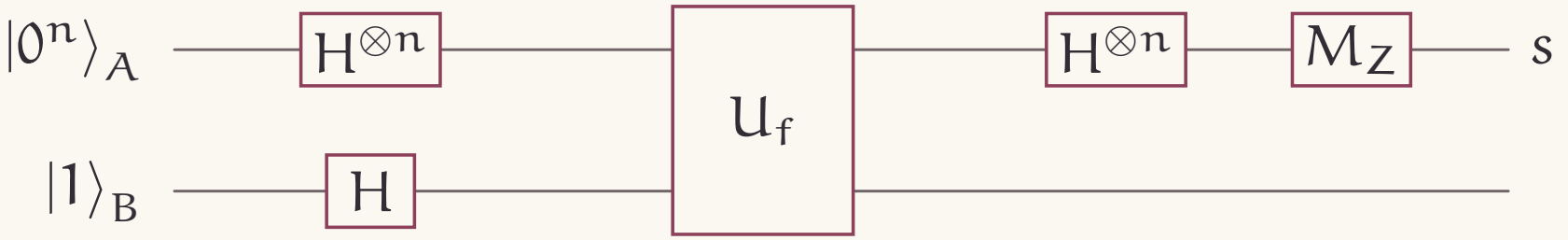
Algoritmi quantistici

Bernstein–Vazirani e Simon



Interferenza e ricostruzione di stringhe nascoste

Marzio De Corato Danilo Bruschi
Dipartimento di Informatica “Giovanni Degli Antoni”
Università degli Studi di Milano

Materiale distribuito con licenza CC BY-NC-SA 4.0.
Revisione del 19 ottobre 2026.

Il percorso del modulo

Una scatola nera riceve un ingresso e restituisce il valore di una funzione. La funzione dipende da una stringa di bit che vogliamo ricostruire. Studiamo due modi in cui questa stringa può essere nascosta e seguiamo i rispettivi procedimenti fino alla risposta.

Bernstein–Vazirani
Ricostruzione dei coefficienti di una parità binaria.

Simon
Ricostruzione della relazione XOR fra ingressi con la stessa uscita.

$$f_s(x) = s \cdot x$$
$$\downarrow$$
Preparazione, oracolo e misura
$$\downarrow$$
$$f(x) = f(x \oplus s)$$

Cominciamo da una stringa di due bit. Le interrogazioni classiche ci mostreranno quale informazione dobbiamo ottenere. Costruiremo poi il circuito quantistico e calcoleremo come la stessa informazione compare nella misura.

Riferimento: N. David Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007, sezioni 2.4–2.5 e Appendice G. Revisione del 19 ottobre 2026. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f.

I coefficienti nascosti di una parità

Cominciamo con una stringa nascosta di due bit, $s = s_1 s_0$. La funzione riceve un ingresso $x = x_1 x_0$ e fa XOR dei bit scelti dai coefficienti di s: un coefficiente uguale a zero esclude la posizione, un coefficiente uguale a uno la include.

$$s = s_1 s_0, \quad x = x_1 x_0, \quad f_s(x) = s_1 x_1 \oplus s_0 x_0.$$
$$s_j = 0 \Rightarrow s_j x_j = 0, \qquad s_j = 1 \Rightarrow s_j x_j = x_j.$$

$s_1 \quad s_0$

↓

Coefficienti che selezionano le posizioni

↓

$s_1 x_1 \oplus s_0 x_0$

Per ricostruire s dobbiamo sapere se la prima posizione partecipa alla parità e se partecipa la seconda. Scegliamo un esempio e cerchiamo gli ingressi che permettono di leggere separatamente queste due informazioni.

$x = x_1 x_0$ è l'ingresso e $s = s_1 s_0$ contiene i due coefficienti cercati. $\oplus$ è XOR: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari.

Dati dell'istanza e informazione disponibile

Scegliamo la stringa $s = 10$: la funzione dell'esempio è quindi $f(x_1x_0) = x_1$. Conosciamo questa scelta per verificare i conti. Chi risolve il problema dispone della scatola nera e deve ricavare i due coefficienti dalle risposte.

x	$f(x)$	$(-1)^{f(x)}$
00	$(1 \cdot 0) \oplus (0 \cdot 0) = 0$	1
01	$(1 \cdot 0) \oplus (0 \cdot 1) = 0$	1
10	$(1 \cdot 1) \oplus (0 \cdot 0) = 1$	-1
11	$(1 \cdot 1) \oplus (0 \cdot 1) = 1$	-1

$$s = 10 \quad \downarrow \quad f_s(x_1x_0) = x_1 \quad \downarrow$$

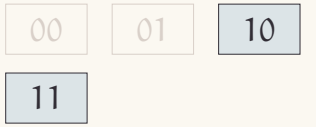
Obiettivo: ricostruire s

Le prime due colonne descrivono le risposte della funzione. L'ultima riporta il segno $(-1)^{f(x)}$, che useremo nel circuito quantistico. Iniziamo con le interrogazioni classiche: scegliamo un ingresso che isoli il primo coefficiente.

In questo esempio $s = 10$ e $f(x_1x_0) = x_1$. Le stringhe seguono l'ordine $00, 01, 10, 11$. Il fattore $(-1)^{f(x)}$ vale $+1$ per uscita 0 e -1 per uscita 1. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Prima interrogazione classica

Per determinare il primo coefficiente, scegliamo un ingresso il cui unico bit uguale a uno occupi quella posizione. Il prodotto con l'altro coefficiente si annulla, perciò la risposta coincide con il coefficiente cercato.



$$f_s(10) = s_1 \cdot 1 \oplus s_0 \cdot 0 = s_1 \oplus 0 = s_1,$$
$$f_{10}(10) = 1 \cdot 1 \oplus 0 \cdot 0 = 1 \oplus 0 = 1.$$

Le stringhe evidenziate soddisfano i vincoli acquisiti.

La risposta 1 determina il primo coefficiente: $s_1 = 1$. Il secondo coefficiente può ancora valere zero oppure uno, quindi restano le stringhe 10 e 11. Scegliamo ora un ingresso che isoli s_0.

$s = s_1 s_0$ è la stringa cercata. Nell'ingresso 10, il primo bit vale 1 e il secondo 0: $f_s(10) = s_1$. Le stringhe evidenziate sono i candidati ancora compatibili. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Seconda interrogazione e ricostruzione

La prima interrogazione ha dato $s_1 = 1$. Con l'ingresso 01 annulliamo il termine contenente s_1 e lasciamo soltanto s_0. La risposta della scatola nera ci fornisce così il coefficiente ancora sconosciuto.

$$f_s(01) = s_1 \cdot 0 \oplus s_0 \cdot 1 = 0 \oplus s_0 = s_0,$$
$$f_{10}(01) = 1 \cdot 0 \oplus 0 \cdot 1 = 0,$$
$$s = (f_s(10), f_s(01)) = (1, 0) = 10.$$

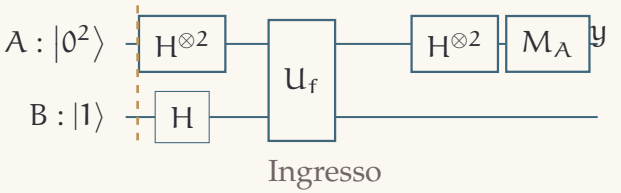
$10 \mapsto 1$
$\downarrow$
$01 \mapsto 0$
$\downarrow$
$s = 10$: due interrogazioni

Le risposte ai due ingressi hanno ricostruito $s = 10$. Nel circuito quantistico prepareremo insieme i quattro ingressi e applicheremo l'oracolo una volta. Dovremo poi trasformare lo stato in modo che la misura renda leggibili entrambi i coefficienti.

Le risposte $f_s(10)$ e $f_s(01)$ restituiscono rispettivamente il primo e il secondo coefficiente. La scrittura $(1, 0)$ indica la stringa di due bit 10. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f.

Il circuito e la funzione dei registri

Usiamo due qubit nel registro A per rappresentare gli ingressi $00, 01, 10, 11$. A sarà anche il registro su cui leggeremo la risposta. Un ulteriore qubit, B, permette di applicare la funzione con un'operazione reversibile: l'oracolo conserva x e fa XOR di $f(x)$ con il contenuto t di B.



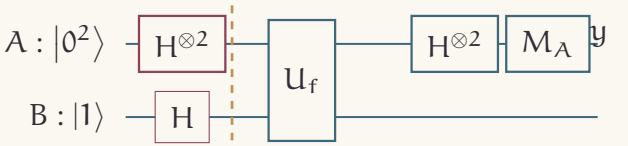
$$|\Psi_0\rangle = |00\rangle_A |1\rangle_B ,$$
$$U_f |x\rangle_A |t\rangle_B = |x\rangle_A |t \oplus f(x)\rangle_B .$$

Prepariamo B in $|1\rangle$. La prima Hadamard lo trasformerà in $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Calcoliamo perché applicare X a questo stato produce il segno che ci serve per codificare $f(x)$.

A contiene due qubit e B un qubit. In $|x\rangle_A |t\rangle_B$, x è l'ingresso e t il bersaglio. $H|1\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. y indicherà il risultato della misura di A. Qubit: sistema con stati di base $|0\rangle, |1\rangle$. Registro: gruppo di qubit. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Reversibile: dall'uscita completa si può ricostruire l'ingresso. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x. Nel circuito, M_A misura A e M_B misura B. La linea oro indica il punto raggiunto.

La preparazione del bersaglio

Prepariamo B in uno stato che cambia di segno quando agisce X.
L'oracolo applica X quando f(x)=1; questa scelta del bersaglio permette quindi di associare un segno al valore della funzione.



Dopo le prime Hadamard

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}0\\ 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ -1\end{pmatrix} = |-\rangle\,,$$

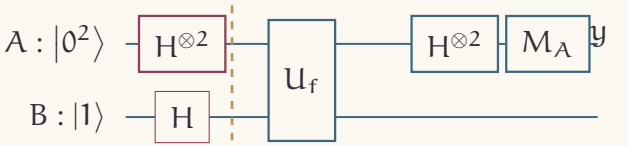
$$X|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1\\ -1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\ 1\end{pmatrix} = -|-\rangle\,.$$

Quando $f(x) = 1$, l'oracolo applica X al bersaglio e il termine con ingresso x acquista un fattore -1. Quando $f(x) = 0$, il bersaglio resta invariato. Prepariamo adesso tutti i registri per applicare questa regola ai quattro ingressi.

$|0\rangle = (1,0)^T$ e $|1\rangle = (0,1)^T$. La porta X scambia $|0\rangle$ e $|1\rangle$: $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Per $f(x) = 0$ agisce l'identità I, che lascia invariato $|-\rangle$. Oracolo: operazione che rende disponibile la funzione f. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La preparazione congiunta

Abbiamo verificato la proprietà del bersaglio. Eseguiamo ora la preparazione completa partendo da $|00\rangle_A |1\rangle_B$: una Hadamard su ciascun qubit di A genera i quattro ingressi e la Hadamard su B prepara $|-\rangle$.



Dopo le prime Hadamard

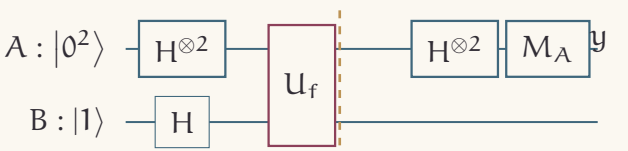
$$
\begin{aligned}
|\Psi_1\rangle &= (H|0\rangle \otimes H|0\rangle) \otimes H|1\rangle \\
&= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |-\rangle \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|-\rangle\,.
\end{aligned}
$$

Ognuno dei quattro ingressi ha ampiezza $1/2$, perché moltiplichiamo due fattori $1/\sqrt{2}$. La somma delle probabilità è $4(1/2)^2 = 1$. L'oracolo può ora applicare la regola dei segni a ciascun termine.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $H|1\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Il simbolo $\otimes$ combina i registri. A parte da $|00\rangle$ e B da $|1\rangle$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'oracolo nell'istanza 10

Applichiamo l'oracolo allo stato appena preparato. La linearità permette di trasformare separatamente i quattro termini e sommarli. Nell'esempio $f(00) = f(01) = 0$ e $f(10) = f(11) = 1$: gli ultimi due ingressi acquistano un segno meno.



Dopo l'oracolo

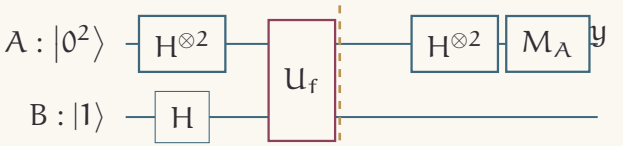
$$
\begin{aligned}
|\Psi_2\rangle &= U_f \left[\tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|-\rangle\right] \\
&= \tfrac{1}{2}\big(U_f\,|00,-\rangle + U_f\,|01,-\rangle + U_f\,|10,-\rangle + U_f\,|11,-\rangle\big) \\
&= \tfrac{1}{2}\big((-1)^0\,|00\rangle + (-1)^0\,|01\rangle + (-1)^1\,|10\rangle + (-1)^1\,|11\rangle\big)\,|-\rangle \\
&= \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)\,|-\rangle\,.
\end{aligned}
$$

I valori della funzione sono diventati segni delle ampiezze di A. Il bersaglio compare come fattore comune $|-\rangle$. Per capire quale operazione debba seguire, calcoliamo che cosa darebbe una misura immediata di A.

$f(x) = x_1$, quindi $f(00), f(01), f(10), f(11) = (0, 0, 1, 1)$. $X^0 = I$ e $X^1 = X$. $|x, -\rangle = |x\rangle_A \otimes |-\rangle_B$, con $X\,|-\rangle = -\,|-\rangle$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Linearità: si trasforma ogni termine dello stato e si sommano i risultati con gli stessi coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La misura prima delle Hadamard finali

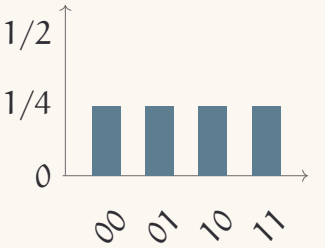
Calcoliamo la distribuzione che si otterrebbe misurando immediatamente A. Questa verifica stabilisce se i segni introdotti dall'oracolo siano già leggibili nella base computazionale.



Prima delle H finali: misura ipotetica

$$|\psi\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle),$$
$$p(00) = p(01) = |1/2|^2 = 1/4,$$
$$p(10) = p(11) = |-1/2|^2 = 1/4, \qquad \sum_y p(y) = 1.$$

Probabilità prima delle Hadamard



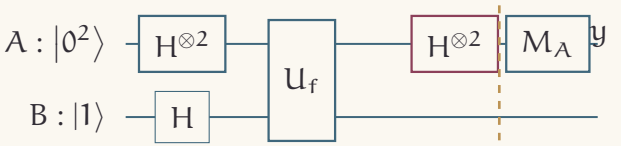
Risultato della misura in A

Tutti i risultati avrebbero probabilità 1/4, perché il quadrato elimina il segno dell'ampiezza. Prima di misurare dobbiamo quindi far sommare i contributi: le Hadamard finali produrranno somme e cancellazioni diverse per ciascuna uscita.

Le ampiezze di A sono $(1, 1, -1, -1)/2$ nell'ordine $00, 01, 10, 11$. La regola di Born dà $p(y) = |A_y|^2$, dove A_y è l'ampiezza dell'esito y. Oracolo: operazione che rende disponibile la funzione f. Base computazionale: gli stati $|00\rangle, |01\rangle, \ldots$ associati alle stringhe lette nella misura. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La matrice delle Hadamard su due bit

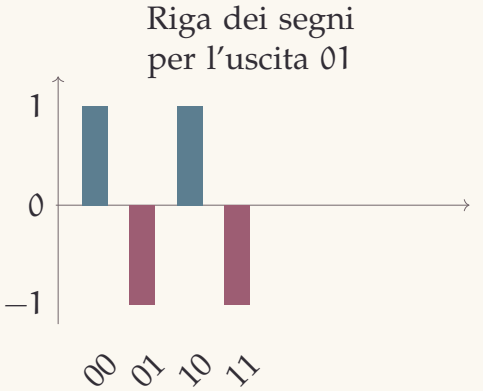
Le Hadamard finali mescolano le quattro ampiezze di A. Costruiamo la matrice che useremo per eseguire queste somme: nel prodotto tensoriale, ogni elemento della prima matrice moltiplica l'intera seconda matrice.



Dopo le Hadamard finali

$$S_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \qquad H = \tfrac{1}{\sqrt{2}} S_2,$$

$$H \otimes H = \tfrac{1}{2} \begin{pmatrix} S_2 & S_2 \\ S_2 & -S_2 \end{pmatrix} = \tfrac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

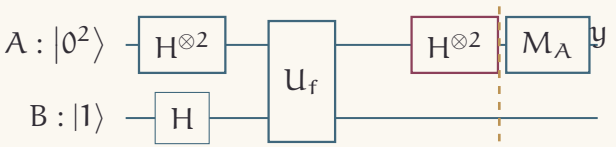


Le righe indicano il possibile risultato y e le colonne l'ingresso x, nell'ordine $00, 01, 10, 11$. La riga $y = 01$, per esempio, pesa i quattro ingressi con $+1, -1, +1, -1$. Moltiplichiamo ogni riga per le ampiezze dello stato dopo l'oracolo.

Righe e colonne seguono l'ordine $00, 01, 10, 11$. Il vettore iniziale è $(1, 1, -1, -1)^T/2$. Il fattore $1/2$ della matrice, moltiplicato per quello del vettore, dà $1/4$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Prodotto tensoriale: combina stati di registri distinti e moltiplica le rispettive ampiezze.

Stringa 10: ampiezze 00 e 01

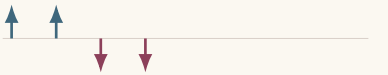
Iniziamo dalle uscite 00 e 01. Il vettore dei segni è $\sigma = (1, 1, -1, -1)$: moltiplichiamo queste componenti per le righe corrispondenti della matrice di Hadamard, quindi sommiamo.



Dopo le Hadamard finali

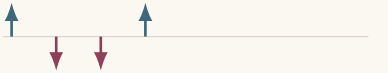
$$\begin{aligned} \mathbf{r}_{00} &= (1, 1, 1, 1), \\ \sigma \odot \mathbf{r}_{00} &= (1, 1, -1, -1), \\ A_{00} &= \frac{1 + 1 - 1 - 1}{4} = 0. \\ \mathbf{r}_{01} &= (1, -1, 1, -1), \\ \sigma \odot \mathbf{r}_{01} &= (1, -1, -1, 1), \\ A_{01} &= \frac{1 - 1 - 1 + 1}{4} = 0. \end{aligned}$$

Uscita $y = 00$: contributi $\pm 1/4$



Somma delle ampiezze: 0

Uscita $y = 01$: contributi $\pm 1/4$



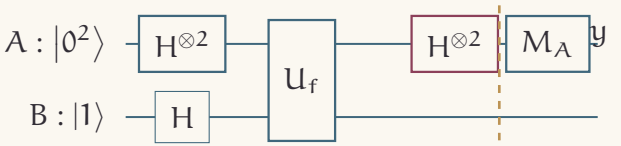
Somma delle ampiezze: 0

Per i risultati 00 e 01 la somma delle ampiezze vale zero. Questi due esiti sono quindi esclusi. Restano da calcolare i contributi alle uscite 10 e 11.

$\sigma = (1, 1, -1, -1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 4. Ordine: $00, 01, 10, 11$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 10: ampiezze 10 e 11

Le uscite fino a 01 sono già state calcolate. Proseguiamo con 10 e 11, conservando $\sigma = (1, 1, -1, -1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 4.



Dopo le Hadamard finali

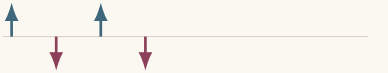
$$\begin{aligned} \mathbf{r}_{10} &= (1, 1, -1, -1), \\ \sigma \odot \mathbf{r}_{10} &= (1, 1, 1, 1), \\ A_{10} &= \frac{1+1+1+1}{4} = 1. \\ \mathbf{r}_{11} &= (1, -1, -1, 1), \\ \sigma \odot \mathbf{r}_{11} &= (1, -1, 1, -1), \\ A_{11} &= \frac{1-1+1-1}{4} = 0. \end{aligned}$$

Uscita $y = 10$: contributi $\pm 1/4$



Somma delle ampiezze: 1

Uscita $y = 11$: contributi $\pm 1/4$



Somma delle ampiezze: 0

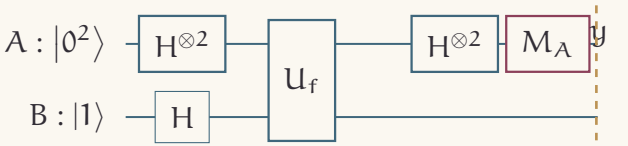
La componente di 10 ha ampiezza uno e quella di 11 ha ampiezza zero. Insieme ai due zeri appena calcolati abbiamo il vettore completo $(0, 0, 1, 0)$. Interpretiamo ora queste ampiezze come probabilità di misura.

$\sigma = (1, 1, -1, -1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 4. Ordine: $00, 01, 10, 11$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

La risposta della prima esecuzione

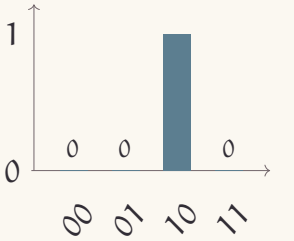
Abbiamo calcolato le ampiezze di tutti e quattro i risultati di A. Applichiamo la regola di Born, che assegna a ciascun esito il modulo quadro della sua ampiezza. Il fattore $|-\rangle_B$ ha norma uno e conserva queste probabilità.

$$(A_{00}, A_{01}, A_{10}, A_{11}) = (0, 0, 1, 0),$$
$$|\Psi_3\rangle = |10\rangle_A |-\rangle_B,$$
$$(p_{00}, p_{01}, p_{10}, p_{11}) = (|0|^2, |0|^2, |1|^2, |0|^2) = (0, 0, 1, 0).$$



Misura di A: risultato y

Probabilità finali



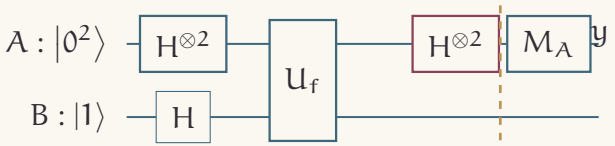
Risultato della misura in A

La misura restituisce 10 con certezza e identifica i due coefficienti. È bastata una chiamata all'oracolo. Torniamo allo stato prima delle Hadamard finali per capire come ciascun qubit abbia prodotto il proprio bit della risposta.

A_y indica l'ampiezza dell'esito y del registro A e $p_y = |A_y|^2$ la sua probabilità. Il registro B è nello stato normalizzato $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Oracolo: operazione che rende disponibile la funzione f. Norma: radice della somma dei moduli quadri dei coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La risposta nei due fattori dello stato di A

Abbiamo già ottenuto la risposta 10. Riprendiamo lo stato di A subito dopo l'oracolo, prima delle Hadamard finali. Raccogliendo i termini lo scriviamo come prodotto di due stati a un qubit e seguiamo separatamente la trasformazione di ciascun fattore.



Dopo le Hadamard finali

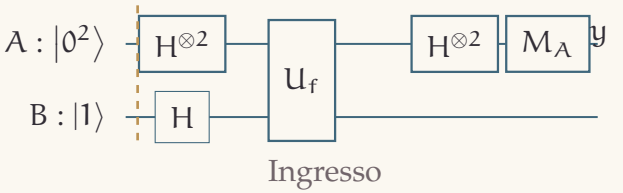
$$\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} = |-\rangle\,|+\rangle\,,$$
$$H\,|-\rangle = \frac{1}{2}[(|0\rangle + |1\rangle) - (|0\rangle - |1\rangle)] = |1\rangle\,,$$
$$H\,|+\rangle = \frac{1}{2}[(|0\rangle + |1\rangle) + (|0\rangle - |1\rangle)] = |0\rangle\,.$$

Il primo fattore è $|-\rangle$ e diventa $|1\rangle$; il secondo è $|+\rangle$ e diventa $|0\rangle$. Ritroviamo così 10. Cambiamo ora il secondo coefficiente da zero a uno e verifichiamo che cosa accade nello stesso circuito.

$|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Le Hadamard danno $H\,|+\rangle = |0\rangle$ e $H\,|-\rangle = |1\rangle$. In questo esempio $s = 10$. Oracolo: operazione che rende disponibile la funzione f. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Entrambi i coefficienti attivi: 11

Manteniamo due qubit e scegliamo s=11, così che entrambi i bit partecipino alla parità. L'esempio verifica come il cambiamento del secondo coefficiente modifichi i segni e la stringa letta alla fine.



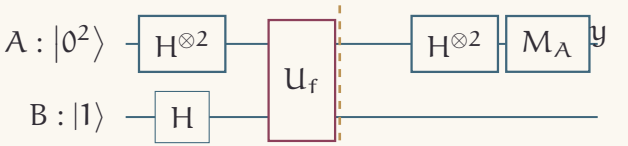
x	$f(x)$	$(-1)^{f(x)}$
00	$(1 \cdot 0) \oplus (1 \cdot 0) = 0$	1
01	$(1 \cdot 0) \oplus (1 \cdot 1) = 1$	-1
10	$(1 \cdot 1) \oplus (1 \cdot 0) = 1$	-1
11	$(1 \cdot 1) \oplus (1 \cdot 1) = 0$	1

Entrambe le posizioni partecipano alla parità. I valori della funzione fissano i segni delle quattro ampiezze: $+1, -1, -1, +1$. Usiamo la stessa preparazione e applichiamo l'oracolo di questa nuova istanza.

In questa istanza $s = s_1 s_0 = 11$, quindi $f(x_1 x_0) = x_1 \oplus x_0$. Lo XOR vale 1 quando i due bit sono diversi e 0 quando sono uguali. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Preparazione e oracolo per 11

Ripresentiamo lo stato iniziale e applichiamo la preparazione. Le righe 01 e 10 della tabella valgono uno e acquistano il segno negativo; le altre conservano il segno positivo.



Dopo l'oracolo

$$|\Psi_0\rangle = |00\rangle\,|1\rangle\,,$$
$$|\Psi_1\rangle = \tfrac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{2}\,|-\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|-\rangle\,,$$
$$|\Psi_2\rangle = \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle)\,|-\rangle\,.$$

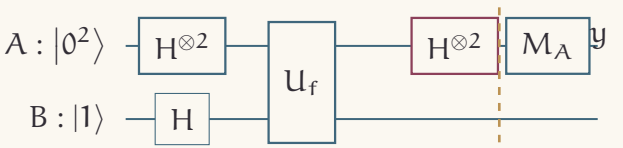
Lo stato dopo l'oracolo ha i quattro segni riportati nella tabella della funzione. Le Hadamard finali useranno la stessa matrice del primo esempio. Calcoliamo le somme per vedere dove si concentra l'ampiezza.

$f(00), f(01), f(10), f(11) = (0, 1, 1, 0)$. Con B in $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, l'oracolo moltiplica ciascun termine per $(-1)^{f(x)}$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Stringa 11: ampiezze 00 e 01

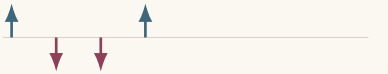
Iniziamo dalle uscite 00 e 01. Il vettore dei segni è $\sigma = (1, -1, -1, 1)$: moltiplichiamo queste componenti per le righe corrispondenti della matrice di Hadamard, quindi sommiamo.

$$\begin{aligned} \mathbf{r}_{00} &= (1, 1, 1, 1), \\ \sigma \odot \mathbf{r}_{00} &= (1, -1, -1, 1), \\ A_{00} &= \frac{1 - 1 - 1 + 1}{4} = 0. \\ \mathbf{r}_{01} &= (1, -1, 1, -1), \\ \sigma \odot \mathbf{r}_{01} &= (1, 1, -1, -1), \\ A_{01} &= \frac{1 + 1 - 1 - 1}{4} = 0. \end{aligned}$$



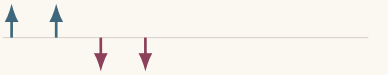
Dopo le Hadamard finali

Uscita $y = 00$: contributi $\pm 1/4$



Somma delle ampiezze: 0

Uscita $y = 01$: contributi $\pm 1/4$



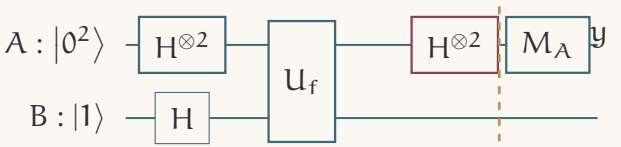
Somma delle ampiezze: 0

Le ampiezze dei risultati 00 e 01 sono entrambe zero. Completiamo la trasformazione calcolando le uscite 10 e 11, che occupano le altre due righe della matrice.

$\sigma = (1, -1, -1, 1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 4. Ordine: $00, 01, 10, 11$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 11: ampiezze 10 e 11

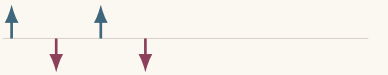
Le uscite fino a 01 sono già state calcolate. Proseguiamo con 10 e 11, conservando $\sigma = (1, -1, -1, 1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 4.



Dopo le Hadamard finali

$$\begin{aligned} \mathbf{r}_{10} &= (1, 1, -1, -1), \\ \sigma \odot \mathbf{r}_{10} &= (1, -1, 1, -1), \\ A_{10} &= \frac{1 - 1 + 1 - 1}{4} = 0. \\ \mathbf{r}_{11} &= (1, -1, -1, 1), \\ \sigma \odot \mathbf{r}_{11} &= (1, 1, 1, 1), \\ A_{11} &= \frac{1 + 1 + 1 + 1}{4} = 1. \end{aligned}$$

Uscita $y = 10$: contributi $\pm 1/4$



Somma delle ampiezze: 0

Uscita $y = 11$: contributi $\pm 1/4$



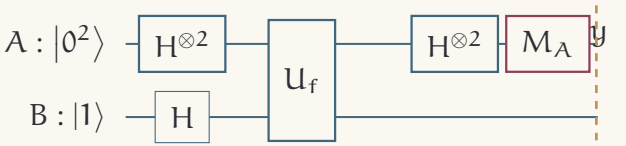
Somma delle ampiezze: 1

Anche l'uscita 10 si annulla. I quattro contributi a 11 hanno invece lo stesso segno e sommano a uno. Abbiamo quindi una sola componente finale non nulla, quella di $|11\rangle$.

$\sigma = (1, -1, -1, 1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 4. Ordine: $00, 01, 10, 11$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Interpretazione della risposta 11

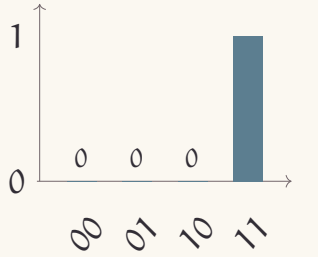
Le somme hanno prodotto un'unica componente non nulla. La fattorizzazione dello stato intermedio chiarisce perché entrambi i qubit della risposta siano ora uguali a uno.



Misura di A: risultato y

Probabilità finali per $s = 11$

$$|\psi\rangle = \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) = |-\rangle\,|-\rangle\,,$$
$$(H \otimes H)\,|\psi\rangle = |1\rangle\,|1\rangle = |11\rangle\,,$$
$$(p_{00}, p_{01}, p_{10}, p_{11}) = (|0|^2, |0|^2, |0|^2, |1|^2) = (0, 0, 0, 1).$$



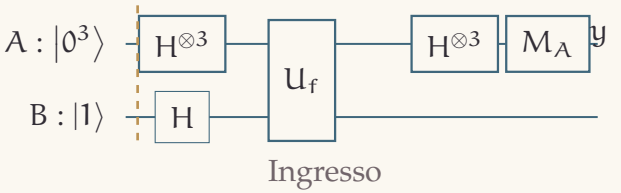
Risultato della misura in A

La misura restituisce 11 e ricostruisce i due coefficienti attivi. Nei due esempi il circuito esterno è rimasto identico. Allunghiamo ora la stringa a tre bit e seguiamo di nuovo il procedimento, dall'interrogazione della funzione fino alla lettura.

In questo esempio $f(x) = x_1 \oplus x_0$ e la stringa cercata è 11. La misura riguarda A. La probabilità di ciascun risultato è il modulo quadro della sua ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Tre coefficienti con due posizioni attive

Consideriamo tre coefficienti nascosti, $s = s_2 s_1 s_0$, e scegliamo l'istanza $s = 101$. Prima di costruire il circuito, fissiamo il costo del metodo classico: ogni ingresso con un solo bit uguale a uno isola il coefficiente nella stessa posizione.



$$f_{101}(100) = 1 \cdot 1 \oplus 0 \cdot 0 \oplus 1 \cdot 0 = 1,$$
$$f_{101}(010) = 1 \cdot 0 \oplus 0 \cdot 1 \oplus 1 \cdot 0 = 0,$$
$$f_{101}(001) = 1 \cdot 0 \oplus 0 \cdot 0 \oplus 1 \cdot 1 = 1.$$

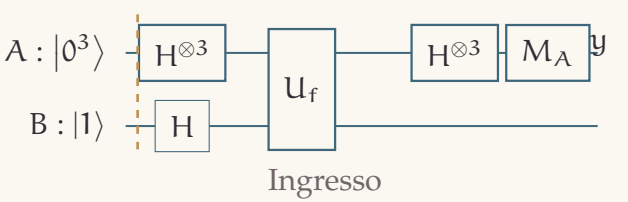
Le tre risposte sono $1, 0, 1$ e ricostruiscono $s = 101$. La funzione fa XOR del primo e dell'ultimo bit dell'ingresso. Scriviamone tutti i valori per controllare i segni che l'oracolo quantistico introdurrà.

L'ingresso è $x = x_2 x_1 x_0$ e la stringa cercata è $s = 101$. La funzione $f(x) = x_2 \oplus x_0$ usa il primo e l'ultimo bit. Il bit centrale non contribuisce. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f.

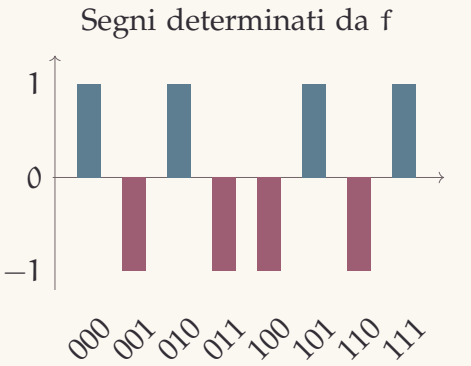
La tabella completa per 101

Valutiamo la funzione su tutti gli otto ingressi. In ogni riga sostituiamo i bit e calcoliamo la parità; la colonna finale anticipa il segno introdotto dall'oracolo.

x	$f(x)$	$(-1)^{f(x)}$
000	$(1\cdot 0)\oplus(0\cdot 0)\oplus(1\cdot 0)=0$	1
001	$(1\cdot 0)\oplus(0\cdot 0)\oplus(1\cdot 1)=1$	-1
010	$(1\cdot 0)\oplus(0\cdot 1)\oplus(1\cdot 0)=0$	1
011	$(1\cdot 0)\oplus(0\cdot 1)\oplus(1\cdot 1)=1$	-1
100	$(1\cdot 1)\oplus(0\cdot 0)\oplus(1\cdot 0)=1$	-1
101	$(1\cdot 1)\oplus(0\cdot 0)\oplus(1\cdot 1)=0$	1
110	$(1\cdot 1)\oplus(0\cdot 1)\oplus(1\cdot 0)=1$	-1
111	$(1\cdot 1)\oplus(0\cdot 1)\oplus(1\cdot 1)=0$	1



Ingresso

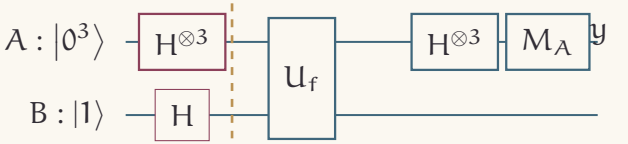


La colonna finale dà i segni $+,-,+,-,-,+,-,+$ nell'ordine da 000 a 111. Prepariamo gli otto ingressi con ampiezze uguali e applichiamo questi segni.

$f(x_2x_1x_0)=x_2\oplus x_0$. Le righe seguono l'ordine da 000 a 111. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1\oplus 1=0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p=|a|^2=a^2$.

La preparazione dei quattro qubit

A ha tre qubit e B resta un singolo qubit. Espandiamo il prodotto della preparazione uniforme, mantenendo visibili tutti gli ingressi che verranno elaborati dall'oracolo.



Dopo le prime Hadamard

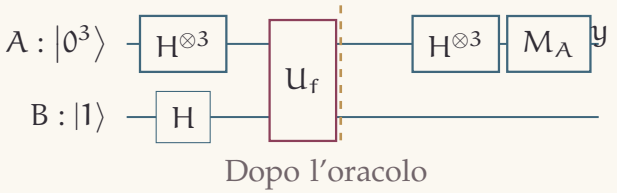
$$
\begin{aligned}
|\Psi_0\rangle &= |000\rangle\,|1\rangle\,, \\
|\Psi_1\rangle &= \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |-\rangle \\
&= \tfrac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle \\
&\quad + |100\rangle + |101\rangle + |110\rangle + |111\rangle)\,|-\rangle\,.
\end{aligned}
$$

Le tre Hadamard su A producono otto termini, ciascuno con ampiezza $1/\sqrt{8}$. La probabilità totale è $8(1/\sqrt{8})^2 = 1$. B è pronto in $|-\rangle$, quindi l'oracolo può trasformare i valori della funzione nei segni della tabella.

A contiene tre qubit inizialmente in $|000\rangle$ e B un qubit inizialmente in $|1\rangle$. Ogni H su A contribuisce un fattore $1/\sqrt{2}$, quindi il prodotto vale $1/\sqrt{8}$. $H|1\rangle_B = |-\rangle_B$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

I segni prodotti dall'oracolo a tre bit

Applichiamo la tabella allo stato uniforme. Ogni termine conserva x; il valore della funzione determina l'azione su B e quindi il segno dell'ampiezza.



Dopo l'oracolo

$$U_f |x, -\rangle = (-1)^{x_2 \oplus x_0} |x, -\rangle ,$$

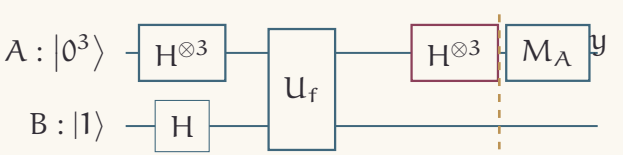
$$|\Psi_2\rangle = \tfrac{1}{\sqrt{8}}(|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle)\,|-\rangle .$$

Il vettore di A contiene ora i segni $+, -, +, -, -, +, -, +$, ciascuno moltiplicato per $1/\sqrt{8}$. Per leggere la stringa nascosta dobbiamo ricombinare queste ampiezze. Costruiamo la matrice delle tre Hadamard finali.

$f(x) = x_2 \oplus x_0$. Il vettore dei segni è $\sigma = (1, -1, 1, -1, -1, 1, -1, 1)$, nell'ordine da 000 a 111. Ogni ampiezza di A è il corrispondente segno diviso per $\sqrt{8}$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La matrice delle Hadamard su tre bit

Poniamo $S_4 = 2H^{\otimes 2}$, la matrice dei segni già calcolata. Da $H^{\otimes 3} = H \otimes H^{\otimes 2}$ otteniamo quattro blocchi: i primi tre sono S_4, l'ultimo è $-S_4$.



Dopo le Hadamard finali

$$H^{\otimes 3} = \frac{1}{\sqrt{8}} \begin{pmatrix} S_4 & S_4 \\ S_4 & -S_4 \end{pmatrix} = \frac{1}{\sqrt{8}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{pmatrix}$$

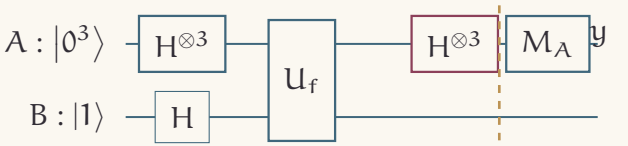
$$S_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Le colonne corrispondono agli ingressi e le righe ai risultati finali, nell'ordine da 000 a 111. Ogni riga moltiplica il vettore dei segni dopo l'oracolo. I due fattori $1/\sqrt{8}$ danno $1/8$ in ciascuna somma.

$S_4 = 2H^{\otimes 2}$. Il prodotto tensoriale usa i blocchi $1S_4, 1S_4, 1S_4, -1S_4$. Ingresso: $(1,-1,1,-1,-1,1,-1,1)^{\mathsf{T}}/\sqrt{8}$. Righe y e colonne x seguono l'ordine $000, 001, 010, 011, 100, 101, 110, 111$. Oracolo: operazione che rende disponibile la funzione f. Prodotto tensoriale: combina stati di registri distinti e moltiplica le rispettive ampiezze.

Stringa 101: ampiezze 000 e 001

Iniziamo dalle uscite 000 e 001. Il vettore dei segni è $\sigma = (1,-1,1,-1,-1,1,-1,1)$: moltiplichiamo queste componenti per le righe corrispondenti della matrice di Hadamard, quindi sommiamo.



Dopo le Hadamard finali

$$\begin{aligned} \mathbf{r}_{000} &= (1,1,1,1,1,1,1,1), \\ \sigma \odot \mathbf{r}_{000} &= (1,-1,1,-1,-1,1,-1,1), \\ A_{000} &= \frac{1-1+1-1-1+1-1+1}{8} = 0. \end{aligned}$$

Uscita $y = 000$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\begin{aligned} \mathbf{r}_{001} &= (1,-1,1,-1,1,-1,1,-1), \\ \sigma \odot \mathbf{r}_{001} &= (1,1,1,1,-1,-1,-1,-1), \\ A_{001} &= \frac{1+1+1+1-1-1-1-1}{8} = 0. \end{aligned}$$

Uscita $y = 001$: contributi $\pm 1/8$



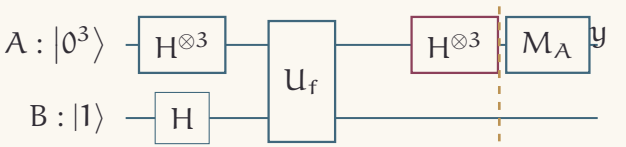
Somma delle ampiezze: 0

I risultati 000 e 001 hanno ampiezza zero. Fin qui nessuna uscita può comparire in misura. Proseguiamo con le due righe della matrice corrispondenti a 010 e 011.

$\sigma = (1,-1,1,-1,-1,1,-1,1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 101: ampiezze 010 e 011

Le uscite fino a 001 sono già state calcolate. Proseguiamo con 010 e 011, conservando $\sigma = (1,-1,1,-1,-1,1,-1,1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\begin{aligned} \mathbf{r}_{010} &= (1,1,-1,-1,1,1,-1,-1),\\ \sigma \odot \mathbf{r}_{010} &= (1,-1,-1,1,-1,1,1,-1),\\ A_{010} &= \frac{1-1-1+1-1+1+1-1}{8} = 0. \end{aligned}$$

Uscita $y = 010$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\begin{aligned} \mathbf{r}_{011} &= (1,-1,-1,1,1,-1,-1,1),\\ \sigma \odot \mathbf{r}_{011} &= (1,1,-1,-1,-1,-1,1,1),\\ A_{011} &= \frac{1+1-1-1-1-1+1+1}{8} = 0. \end{aligned}$$

Uscita $y = 011$: contributi $\pm 1/8$



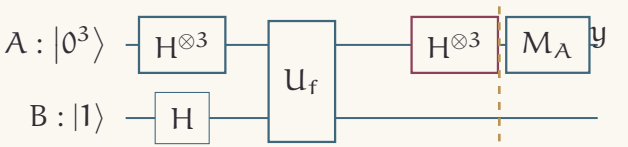
Somma delle ampiezze: 0

Anche i risultati 010 e 011 si annullano. Abbiamo controllato le prime quattro uscite. Passiamo alle stringhe che iniziano con uno, mantenendo lo stesso vettore di ingresso e lo stesso fattore 1/8.

$\sigma = (1,-1,1,-1,-1,1,-1,1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 101: ampiezze 100 e 101

Le uscite fino a 011 sono già state calcolate. Proseguiamo con 100 e 101, conservando $\sigma = (1,-1,1,-1,-1,1,-1,1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\begin{aligned} r_{100} &= (1,1,1,1,-1,-1,-1,-1),\\ \sigma \odot r_{100} &= (1,-1,1,-1,1,-1,1,-1),\\ A_{100} &= \frac{1-1+1-1+1-1+1-1}{8} = 0. \end{aligned}$$

Uscita $y = 100$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\begin{aligned} r_{101} &= (1,-1,1,-1,-1,1,-1,1),\\ \sigma \odot r_{101} &= (1,1,1,1,1,1,1,1),\\ A_{101} &= \frac{1+1+1+1+1+1+1+1}{8} = 1. \end{aligned}$$

Uscita $y = 101$: contributi $\pm 1/8$



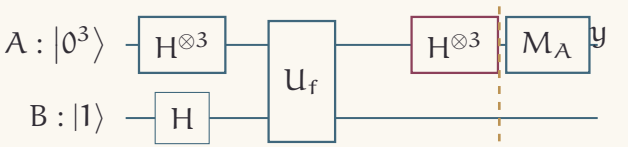
Somma delle ampiezze: 1

Per 100 i contributi si cancellano. Per 101 tutti gli otto contributi sommano a uno: compare la stringa cercata. Completiamo comunque il vettore finale controllando che le uscite 110 e 111 si annullino.

$\sigma = (1,-1,1,-1,-1,1,-1,1)$ contiene i segni dopo l'oracolo. r_y è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 101: ampiezze 110 e 111

Le uscite fino a 101 sono già state calcolate. Proseguiamo con 110 e 111, conservando $\sigma = (1,-1,1,-1,-1,1,-1,1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\begin{aligned} r_{110} &= (1,1,-1,-1,-1,-1,1,1), \\ \sigma \odot r_{110} &= (1,-1,-1,1,1,-1,-1,1), \\ A_{110} &= \frac{1-1-1+1+1-1-1+1}{8} = 0. \end{aligned}$$

Uscita $y = 110$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\begin{aligned} r_{111} &= (1,-1,-1,1,-1,1,1,-1), \\ \sigma \odot r_{111} &= (1,1,-1,-1,1,1,-1,-1), \\ A_{111} &= \frac{1+1-1-1+1+1-1-1}{8} = 0. \end{aligned}$$

Uscita $y = 111$: contributi $\pm 1/8$



Somma delle ampiezze: 0

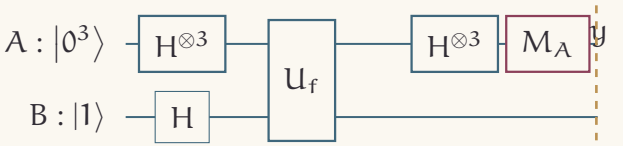
Le ultime due ampiezze valgono zero. Il vettore completo ha quindi ampiezza uno soltanto sulla componente 101. Possiamo ora applicare Born a tutte le uscite e concludere l'esecuzione.

$\sigma = (1,-1,1,-1,-1,1,-1,1)$ contiene i segni dopo l'oracolo. r_y è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Distribuzione finale e lettura di 101

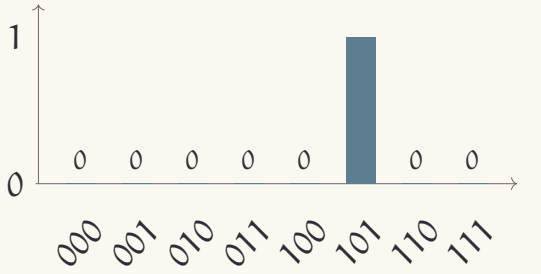
Riuniamo le ampiezze nell'ordine della base. Il controllo della norma e la regola di Born verificano che la misura sia deterministica e che i bit osservati abbiano il significato dei coefficienti cercati.

$$
\begin{aligned}
(A_{000}, A_{001}, A_{010}, A_{011}, A_{100}, A_{101}, A_{110}, A_{111}) \\
&= (0,0,0,0,0,1,0,0), \\
|\Psi_3\rangle = |101\rangle\,|-\rangle\,, \quad p(101) = 1, \quad p(y \neq 101) &= 0, \\
\sum_y p(y) = |1|^2 + 7|0|^2 &= 1.
\end{aligned}
$$



Misura di A: risultato y

Probabilità finali



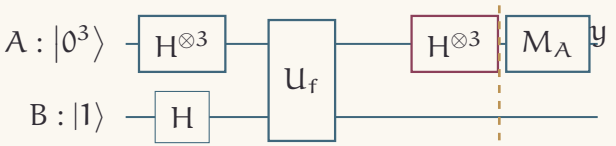
Risultato della misura in A

La misura restituisce 101 con certezza. Riprendiamo lo stato dopo l'oracolo per leggerne la struttura: i tre fattori a un qubit spiegheranno come ciascuna posizione produce il bit corrispondente della risposta.

A_y è l'ampiezza dell'esito y di A e $p_y = |A_y|^2$. L'ordine delle componenti è 000, 001, 010, 011, 100, 101, 110, 111. La funzione dell'esempio è $f(x) = x_2 \oplus x_0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Norma: radice della somma dei moduli quadri dei coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La fattorizzazione dei segni di 101

Abbiamo già ottenuto 101 dalle otto somme. Torniamo allo stato di A dopo l'oracolo per spiegare la stessa risposta bit per bit. I segni dipendono dal primo e dall'ultimo bit dell'ingresso: queste posizioni danno un fattore $|-\rangle$, mentre quella centrale dà $|+\rangle$.



Dopo le Hadamard finali

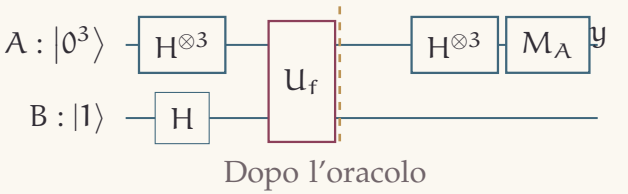
$$
\begin{aligned}
|-\rangle\,|+\rangle\,|-\rangle &= \tfrac{1}{\sqrt{8}}(|0\rangle - |1\rangle)(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\
&= \tfrac{1}{\sqrt{8}}(|00\rangle + |01\rangle - |10\rangle - |11\rangle)(|0\rangle - |1\rangle) \\
&= \tfrac{1}{\sqrt{8}}(|000\rangle - |001\rangle + |010\rangle - |011\rangle \\
&\quad - |100\rangle + |101\rangle - |110\rangle + |111\rangle), \\
H^{\otimes 3}\,|-\rangle\,|+\rangle\,|-\rangle &= |1\rangle\,|0\rangle\,|1\rangle\,.
\end{aligned}
$$

Le tre Hadamard trasformano $|-\rangle\,|+\rangle\,|-\rangle$ in $|1\rangle\,|0\rangle\,|1\rangle$. Possiamo riconoscere questo comportamento anche nella realizzazione dell'oracolo mediante porte CNOT. Apriamo quindi il circuito dell'istanza 101 per studiarne la struttura.

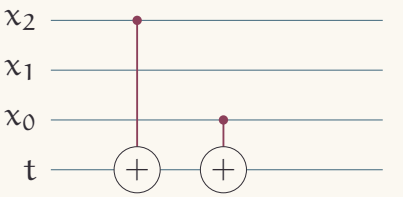
$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Le identità $H\,|+\rangle = |0\rangle$ e $H\,|-\rangle = |1\rangle$ si applicano a ciascun qubit. I prodotti dei ket sono prodotti tensoriali. Oracolo: operazione che rende disponibile la funzione f. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1. Prodotto tensoriale: combina stati di registri distinti e moltiplica le rispettive ampiezze. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Una realizzazione dell'oracolo per 101

Per la funzione $f(x) = x_2 \oplus x_0$, due CNOT aggiungono al bersaglio prima x_2 e poi x_0. Mostriamo questa costruzione per verificare l'istanza. Il procedimento di ricerca riceve invece U_f come operazione disponibile e ne ricava i coefficienti attraverso il circuito.



Dopo l'oracolo



Realizzazione dell'istanza scelta. L'algoritmo riceve U_f come operazione disponibile.

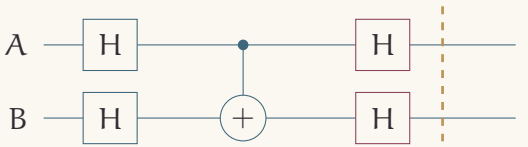
$$
\begin{aligned}
|x_2x_1x_0\rangle\,|t\rangle &\longmapsto |x_2x_1x_0\rangle\,|t \oplus x_2\rangle \\
&\longmapsto |x_2x_1x_0\rangle\,|t \oplus x_2 \oplus x_0\rangle \\
&= |x\rangle\,|t \oplus f_{101}(x)\rangle\,.
\end{aligned}
$$

Le Hadamard prima e dopo una CNOT permettono di scambiare controllo e bersaglio. Verifichiamo questa identità su due qubit: ci consentirà poi di vedere la risposta scritta direttamente sui fili di A.

Una CNOT controllata da a aggiorna il bersaglio b: $|a, b\rangle \mapsto |a, b \oplus a\rangle$. Qui le posizioni di controllo sono x_2 e x_0, perché $f(x) = x_2 \oplus x_0$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'inversione della CNOT: 00 e 01

Isoliamo due soli qubit, che qui chiamiamo A e B. Vogliamo verificare $(H \otimes H)C_{A\to B}(H \otimes H) = C_{B\to A}$. Seguiamo le operazioni sugli ingressi 00 e 01: prima le due Hadamard, poi la CNOT, infine le somme delle Hadamard finali.

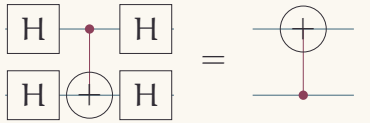


Identità su due qubit: dopo le ultime H

$$|00\rangle \xrightarrow{H\otimes H} \tfrac{1}{2}(1,1,1,1)^T \xrightarrow{C_{A\to B}} \tfrac{1}{2}(1,1,1,1)^T,$$

$$|01\rangle \xrightarrow{H\otimes H} \tfrac{1}{2}(1,-1,1,-1)^T \xrightarrow{C_{A\to B}} \tfrac{1}{2}(1,-1,-1,1)^T,$$

Ingresso	A_{00}	A_{01}	A_{10}	A_{11}
00	$\frac{1+1+1+1}{4} = 1$	$\frac{1-1+1-1}{4} = 0$	$\frac{1+1-1-1}{4} = 0$	$\frac{1-1-1+1}{4} = 0$
01	$\frac{1-1-1+1}{4} = 0$	$\frac{1+1-1-1}{4} = 0$	$\frac{1-1+1-1}{4} = 0$	$\frac{1+1+1+1}{4} = 1$



La coniugazione con $H \otimes H$ scambia controllo e bersaglio.

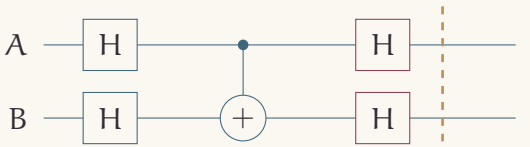
$$|00\rangle \longmapsto |00\rangle, \quad |01\rangle \longmapsto |11\rangle$$

Otteniamo $00 \mapsto 00$ e $01 \mapsto 11$, come quando B controlla A. Restano gli ingressi 10 e 11. Il controllo su tutti i vettori della base stabilirà l'identità per qualsiasi sovrapposizione.

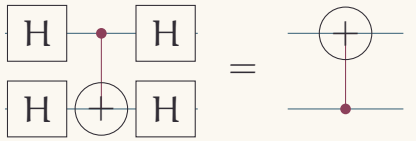
$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. $C_{A\to B}|a,b\rangle = |a, b \oplus a\rangle$ e $C_{B\to A}|a,b\rangle = |a \oplus b, b\rangle$. Nella tabella A_y è l'ampiezza finale dell'esito y per l'ingresso della riga. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1. Sovrapposizione: somma di stati, ciascuno pesato dalla propria ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'inversione della CNOT: 10 e 11

Completiamo la verifica con i vettori 10 e 11. Il procedimento è quello della slide precedente: prima le Hadamard, poi la permutazione della CNOT, infine le quattro somme della trasformazione finale.



Identità su due qubit: dopo le ultime H



La coniugazione con $H \otimes H$ scambia controllo e bersaglio.

$$|10\rangle \xrightarrow{H\otimes H} \tfrac{1}{2}(1,1,-1,-1)^T \xrightarrow{C_{A\to B}} \tfrac{1}{2}(1,1,-1,-1)^T,$$
$$|11\rangle \xrightarrow{H\otimes H} \tfrac{1}{2}(1,-1,-1,1)^T \xrightarrow{C_{A\to B}} \tfrac{1}{2}(1,-1,1,-1)^T,$$

Ingresso	A_{00}	A_{01}	A_{10}	A_{11}
10	$\frac{1+1-1-1}{4} = 0$	$\frac{1-1-1+1}{4} = 0$	$\frac{1+1+1+1}{4} = 1$	$\frac{1-1+1-1}{4} = 0$
11	$\frac{1-1+1-1}{4} = 0$	$\frac{1+1+1+1}{4} = 1$	$\frac{1-1-1+1}{4} = 0$	$\frac{1+1-1-1}{4} = 0$

$$|10\rangle \longmapsto |10\rangle\,, \quad |11\rangle \longmapsto |01\rangle$$

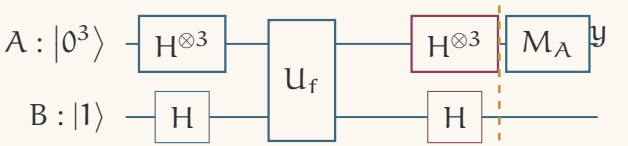
I risultati dei quattro ingressi coincidono con quelli della CNOT controllata da B. Ogni stato è una loro combinazione, quindi la linearità estende l'uguaglianza a ogni stato. Torniamo all'istanza 101.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. $C_{A\to B}|a,b\rangle = |a, b \oplus a\rangle$ e $C_{B\to A}|a,b\rangle = |a \oplus b, b\rangle$. Nella tabella A_y è l'ampiezza finale dell'esito y per l'ingresso della riga. Linearità: si trasforma ogni termine dello stato e si sommano i risultati con gli stessi coefficienti. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

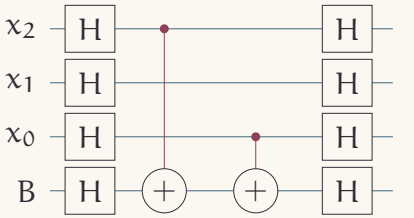
La coniugazione di due CNOT

Torniamo ai quattro qubit: tre nel registro A e uno in B. Aggiungiamo una Hadamard finale anche su B per applicare l'identità appena verificata. Questa porta agisce soltanto sul bersaglio e conserva le probabilità della misura di A. Chiamiamo $K = H^{\otimes 4}$ il prodotto delle quattro Hadamard.

$$K = H^{\otimes 4}, \quad K^2 = I, \quad U_f = C_{0\to B} C_{2\to B},$$
$$K U_f K = K C_{0\to B} (KK) C_{2\to B} K$$
$$= (K C_{0\to B} K)(K C_{2\to B} K) = C_{B\to 0} C_{B\to 2}.$$



Circuito equivalente: H finale anche su B



Circuito con H finale aggiunta su B. Le H iniziali e finali formano $K = H^{\otimes 4}$.

Inserendo $K^2 = I$ fra le due CNOT possiamo trasformarle una alla volta. Ogni coppia di Hadamard scambia controllo e bersaglio: B diventa il controllo che agisce sulle posizioni 2 e 0 di A. Seguiamo questo circuito equivalente dallo stato iniziale.

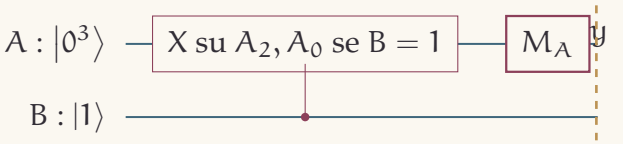
$K = H_A^{\otimes 3} \otimes H_B$ applica H a tutti e quattro i qubit. Poiché $H^2 = I$, anche $K^2 = I$. Nei prodotti di operatori agisce prima il fattore più a destra. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1.

La risposta nel circuito equivalente

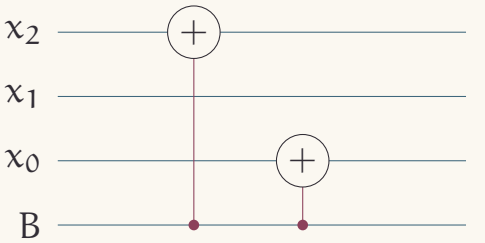
Applichiamo il circuito equivalente a 000 nel registro A e 1 in B. Il valore uno del controllo attiva entrambe le CNOT invertite, che modificano le posizioni selezionate dalla stringa.

$$|000\rangle_A |1\rangle_B \xrightarrow{C_{B\to 2}} |100\rangle_A |1\rangle_B \xrightarrow{C_{B\to 0}} |101\rangle_A |1\rangle_B ,$$

senza l'ultima H su B: $|101\rangle_A |-\rangle_B$.



Circuito equivalente: lettura di A



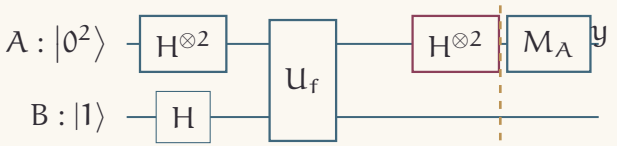
B resta 1: $000 \to 100 \to 101$.
Controlli e bersagli sono scambiati.

Il controllo B vale uno, quindi le due CNOT capovolgono il primo e l'ultimo bit di A: $000 \mapsto 100 \mapsto 101$. Ritroviamo la risposta. Per descrivere il procedimento con una lunghezza arbitraria introduciamo ora una formula unica per i coefficienti delle Hadamard.

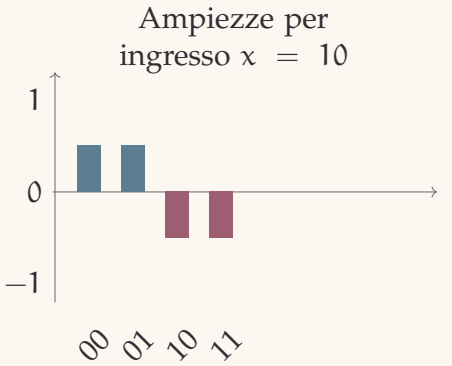
$C_{B\to j}$ inverte il qubit x_j quando B vale 1. L'ordine dei bit di A è $x_2x_1x_0$. La H aggiunta in fondo a B scambia $|-\rangle$ e $|1\rangle$. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'indice di uscita nella trasformazione di Hadamard

Vogliamo esprimere le trasformazioni già calcolate con una formula valida per qualsiasi numero di bit. Introduciamo prima la notazione su un ingresso a due bit, $x = 10$. La lettera y enumera i quattro termini di base nella trasformata di questo ingresso.



Formula delle H finali: un ingresso



y	$10 \cdot y$	$(-1)^{10 \cdot y}$
00	$1 \cdot 0 \oplus 0 \cdot 0 = 0$	$+1$
01	$1 \cdot 0 \oplus 0 \cdot 1 = 0$	$+1$
10	$1 \cdot 1 \oplus 0 \cdot 0 = 1$	-1
11	$1 \cdot 1 \oplus 0 \cdot 1 = 1$	-1

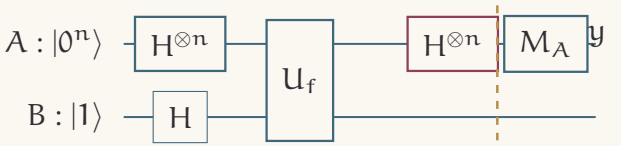
$$H^{\otimes 2}|10\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle).$$

Per ogni possibile risultato y, il prodotto binario $10 \cdot y$ determina il segno del suo coefficiente. Con n bit avremo 2^n termini. Ricaviamo ora tutti i loro coefficienti dal prodotto delle singole Hadamard.

$x = 10$ è l'ingresso trasformato. y percorre $00, 01, 10, 11$. Il prodotto binario $x \cdot y = x_1 y_1 \oplus x_0 y_0$ determina il segno del coefficiente. XOR ($\oplus$): somma modulo 2, con $1 \oplus 1 = 0$. Ampiezza: coefficiente del ket. Il ket $|y\rangle$ indica lo stato associato alla stringa y.

La formula delle Hadamard sui bit

Il caso $x = 10$ ha mostrato il ruolo dell'indice y. Manteniamo ora fissata un'intera stringa $x = x_{n-1} \cdots x_0$: ciascun y_j percorre separatamente 0 e 1, e tutte le combinazioni formano $y \in \{0,1\}^n$. Espandiamo il prodotto delle trasformazioni dei singoli qubit.



Formula delle H finali sui singoli bit

$$H|x_j\rangle = \frac{|0\rangle + (-1)^{x_j}|1\rangle}{\sqrt{2}} = 2^{-1/2}\sum_{y_j=0}^{1}(-1)^{x_j y_j}|y_j\rangle\,,$$

$$H^{\otimes n}|x\rangle = 2^{-n/2}\sum_{y_{n-1},\ldots,y_0}\prod_j(-1)^{x_j y_j}|y_{n-1}\cdots y_0\rangle$$

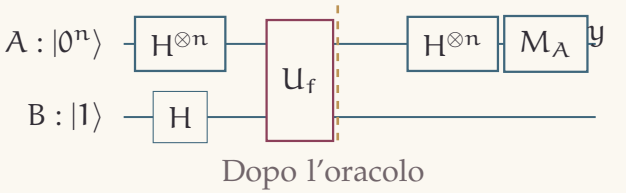
$$= 2^{-n/2}\sum_y(-1)^{x\cdot y}|y\rangle\,.$$

Ogni posizione in cui sia x_j sia y_j valgono uno introduce un segno meno. Il prodotto binario conta la parità di questi segni, e il fattore $1/\sqrt{2^n}$ viene dalle n Hadamard. Usiamo la formula per seguire il circuito di Bernstein–Vazirani con n coefficienti.

$H|x_j\rangle = (|0\rangle + (-1)^{x_j}|1\rangle)/\sqrt{2}$. $x \cdot y$ è lo XOR dei prodotti dei bit nella stessa posizione. La somma su y percorre tutte le stringhe di n bit. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Lo stato per una stringa di lunghezza n

Gli esempi hanno mostrato la dipendenza dei segni dai coefficienti. Scriviamo la preparazione per un numero arbitrario di bit e applichiamo la linearità dell'oracolo, mantenendo esplicito il fattore comune del bersaglio.



Dopo l'oracolo

$$|\Psi_0\rangle = |0^n\rangle\,|1\rangle\,, \quad |\Psi_1\rangle = 2^{-n/2}\sum_x |x\rangle\,|-\rangle\,,$$
$$U_f\,|x,-\rangle = (-1)^{s\cdot x}\,|x,-\rangle\,,$$
$$|\Psi_2\rangle = 2^{-n/2}\sum_x (-1)^{s\cdot x}\,|x\rangle\,|-\rangle\,.$$

Dopo l'oracolo il termine con ingresso x ha ampiezza $(-1)^{s\cdot x}/\sqrt{2^n}$. Le Hadamard finali aggiungeranno il fattore $(-1)^{x\cdot y}/\sqrt{2^n}$ per il risultato y. Sommiamo questi contributi su tutti gli ingressi.

A contiene n qubit e B un qubit. 0^n è la stringa di n zeri. $f_s(x) = s\cdot x$ e $U_f\,|x\rangle\,|-\rangle = (-1)^{s\cdot x}\,|x\rangle\,|-\rangle$. La somma su x percorre tutti i 2^n ingressi. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Linearità: si trasforma ogni termine dello stato e si sommano i risultati con gli stessi coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

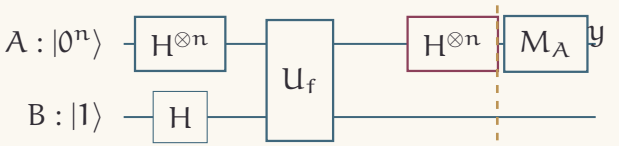
Il coefficiente di una singola uscita

Per ottenere la probabilità di una particolare uscita y raccogliamo tutti i contributi che conducono al suo vettore di base. Applichiamo la formula delle Hadamard a ciascun termine e riordiniamo due somme finite.

$$|\Psi_3\rangle = 2^{-n/2} \sum_x (-1)^{s\cdot x} \left[2^{-n/2} \sum_y (-1)^{x\cdot y} |y\rangle \right] |-\rangle$$

$$= \sum_y \left[2^{-n} \sum_x (-1)^{s\cdot x + x\cdot y} \right] |y\rangle\,|-\rangle\,,$$

$$A_y = 2^{-n} \sum_x (-1)^{(s\oplus y)\cdot x}.$$



Dopo le Hadamard finali

	00	01	10	11
x = 00	±	±	±	±
x = 01	±	±	±	±
x = 10	±	±	±	±
x = 11	±	±	±	±

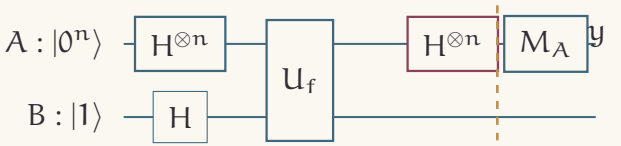
Una colonna raccoglie tutti gli ingressi che contribuiscono allo stesso y.

Per ottenere l'ampiezza di un risultato y dobbiamo sommare i contributi di tutti gli ingressi x. Il segno dipende dai bit di $s \oplus y$. Separiamo ora la somma in fattori, uno per ciascuna posizione, per capire quando il risultato si annulla.

x è l'ingresso e y il risultato finale di A. A_y è il coefficiente di $|y\rangle_A$. Per bit a e b, $(-1)^{a+b} = (-1)^{a\oplus b}$. Il bersaglio B resta nel fattore comune $|-\rangle$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La fattorizzazione della somma

Poniamo $r = s \oplus y$. I segni dei singoli bit si moltiplicano: $(-1)^{r\cdot x} = \prod_j (-1)^{r_j x_j}$. Svolgiamo la somma per due bit, poi raccogliamo un fattore per ogni posizione.



Dopo le Hadamard finali

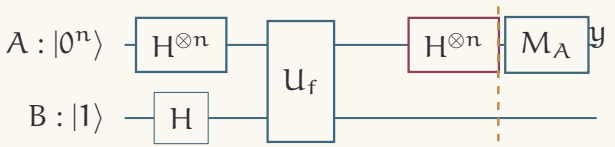
$$\sum_{x_1,x_0} (-1)^{r_1 x_1}(-1)^{r_0 x_0}$$
$$= (1)(1) + (1)(-1)^{r_0} + (-1)^{r_1}(1) + (-1)^{r_1}(-1)^{r_0}$$
$$= [1 + (-1)^{r_1}][1 + (-1)^{r_0}],$$
$$\sum_{x_{n-1}=0}^{1} \cdots \sum_{x_0=0}^{1} \prod_j (-1)^{r_j x_j} = \prod_j [1 + (-1)^{r_j}].$$

Ogni bit di x ha due scelte, zero e uno. La somma si fattorizza quindi nei termini $1 + (-1)^{s_j \oplus y_j}$. Calcoliamo un fattore quando i due bit coincidono e quando differiscono.

$r = s \oplus y$ confronta bit per bit la stringa cercata con il possibile risultato. $r \cdot x = \bigoplus_j r_j x_j$. Ogni bit x_j può valere 0 oppure 1, indipendentemente dagli altri. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

I fattori che selezionano la stringa

Se il bit di y coincide con quello di s, il relativo fattore vale due. Se i bit differiscono, i due contributi si cancellano. Una sola differenza annulla l'intero prodotto che determina l'ampiezza.



Dopo le Hadamard finali

s_j	y_j	$s_j \oplus y_j$	$1 + (-1)^{s_j \oplus y_j}$
0	0	0	$1 + 1 = 2$
0	1	1	$1 - 1 = 0$
1	0	1	$1 - 1 = 0$
1	1	0	$1 + 1 = 2$

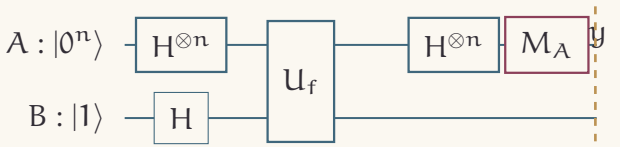
$$A_y = 2^{-n} \prod_{j=0}^{n-1} [1 + (-1)^{s_j \oplus y_j}].$$

Basta una posizione con $y_j \neq s_j$ per introdurre un fattore zero e annullare l'ampiezza. Se tutti i bit coincidono, i n fattori valgono due e il prodotto 2^n cancella il denominatore. Rimane quindi soltanto il risultato $y = s$.

Il bit $r_j = s_j \oplus y_j$ vale 0 se i due bit coincidono e 1 se sono diversi. Il fattore corrispondente è $1 + (-1)^{r_j}$ e vale rispettivamente 2 oppure 0. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

La conclusione della dimostrazione

Inseriamo i due possibili valori del prodotto nella formula dell'ampiezza. Le normalizzazioni compensano il fattore ottenuto quando tutte le posizioni coincidono.



$$y = s: \quad A_s = 2^{-n} \underbrace{2 \cdot 2 \cdots 2}_{n \text{ fattori}} = 2^{-n} 2^n = 1,$$

$$y \neq s: \quad A_y = 2^{-n} \cdot 0 = 0,$$

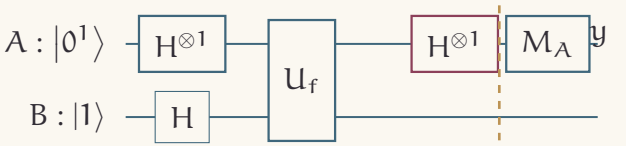
$$|\Psi_3\rangle = |s\rangle\,|-\rangle\,, \quad p(s) = |1|^2 = 1, \quad p(y \neq s) = 0.$$

La misura di A restituisce la stringa nascosta con certezza, come nei casi a due e tre bit. Il circuito usa una sola chiamata all'oracolo. Verifichiamo il risultato nel caso minimo di un bit e quando tutti i coefficienti sono zero.

A_y è l'ampiezza del risultato y di A e $p(y) = |A_y|^2$. Nella famiglia $f_s(x) = s \cdot x$, s contiene i coefficienti della parità. B resta nello stato normalizzato $|-\rangle$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Il caso minimo: un coefficiente

Per n=1 e s=1 la funzione è f(x)=x. Verifichiamo la selezione mediante la matrice di Hadamard, così da controllare il limite minimo della famiglia.



Dopo le Hadamard finali

$$|0\rangle\,|1\rangle \longmapsto \tfrac{|0\rangle+|1\rangle}{\sqrt{2}}\,|-\rangle \xrightarrow{U_f} \tfrac{|0\rangle-|1\rangle}{\sqrt{2}}\,|-\rangle\,,$$

$$H\tfrac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \tfrac{1}{2}\begin{pmatrix}1-1\\1+1\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle\,,$$

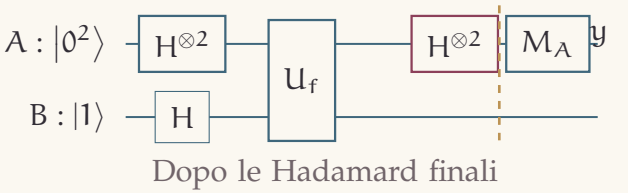
$$p(0) = |0|^2 = 0, \qquad p(1) = |1|^2 = 1.$$

Con un solo coefficiente, l'ingresso classico 1 restituisce già s. Entrambi i procedimenti richiedono quindi una chiamata alla funzione. Il calcolo quantistico continua a dare la risposta prevista dalla formula generale.

Con n=1, ingresso x e coefficiente s sono singoli bit. $H|+\rangle = |0\rangle$ e $H|-\rangle = |1\rangle$, con $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

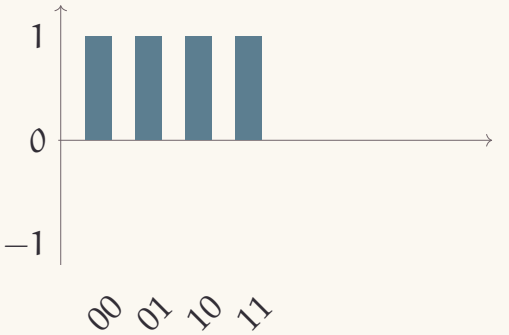
La stringa nulla: preparazione e somme

Consideriamo n=2 e s=00. La funzione vale zero su tutti gli ingressi, perciò l'oracolo conserva i segni della preparazione. Calcoliamo tutte le ampiezze per interpretare l'uscita nulla.



Dopo le Hadamard finali

Ampiezze in unità 1/2



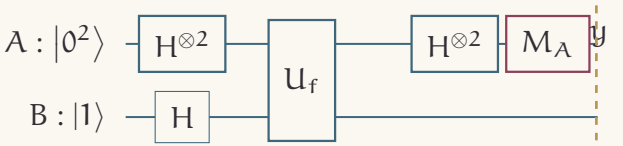
$$|\Psi_0\rangle = |00\rangle\,|1\rangle\,, \quad |\Psi_1\rangle = \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\,|-\rangle\,,$$
$$f_s(x) = 0x_1 \oplus 0x_0 = 0 \Rightarrow U_f = I, \quad |\Psi_2\rangle = |\Psi_1\rangle\,,$$
$$A_{00} = (1+1+1+1)/4 = 1, \quad A_{01} = (1-1+1-1)/4 = 0,$$
$$A_{10} = (1+1-1-1)/4 = 0, \quad A_{11} = (1-1-1+1)/4 = 0.$$

Quando $s = 0^n$, la funzione vale zero per ogni ingresso e l'oracolo lascia tutte le ampiezze positive. Le Hadamard finali riportano ogni fattore $|+\rangle$ in $|0\rangle$. Interpretiamo la stringa nulla che compare nella misura.

Con $s = 00$, $f(x) = 0$ per tutti i quattro ingressi e i segni sono $(1, 1, 1, 1)$. Le componenti seguono l'ordine $00, 01, 10, 11$. I due fattori $1/2$ danno il denominatore 4 nelle somme. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'interpretazione dell'uscita nulla

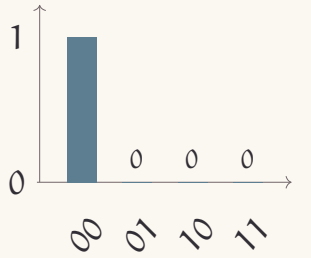
Riprendiamo il vettore finale per s=00 e calcoliamo le probabilità. La stringa osservata identifica precisamente una funzione della famiglia e costituisce una risposta completa al problema.



Misura di A: risultato y

Probabilità finali per $s = 00$

$$(A_{00}, A_{01}, A_{10}, A_{11}) = (1, 0, 0, 0),$$
$$(p_{00}, p_{01}, p_{10}, p_{11}) = (1^2, 0^2, 0^2, 0^2) = (1, 0, 0, 0),$$
$$s = 00 \quad \Longrightarrow \quad f_s(x) = 0 \quad \text{per ogni } x.$$



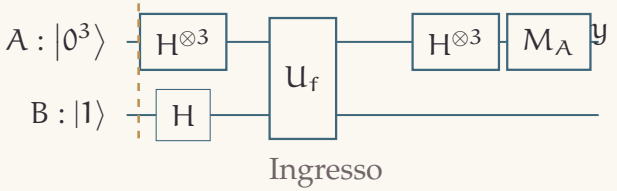
Risultato della misura in A

Nel problema di Bernstein–Vazirani la stringa nulla è una risposta ammessa: indica che nessuna posizione partecipa alla parità. Consideriamo ora una funzione in cui, oltre ai coefficienti, compare un bit costante b da aggiungere mediante XOR.

Qui A contiene due qubit e si misura dopo le Hadamard finali. Il risultato 00 ricostruisce la stringa nulla, ammessa nel problema di Bernstein–Vazirani. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

L'estensione affine della famiglia

Aggiungiamo il bit costante b: $f_{s,b}(x) = s \cdot x \oplus b$. Con $s = 011$ e $b = 1$ otteniamo $f(x) = x_1 \oplus x_0 \oplus 1$. Calcoliamone tutti i valori.



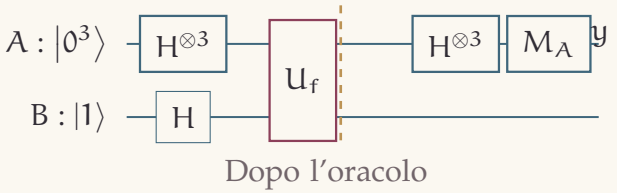
x	$f(x)$	$(-1)^{f(x)}$
000	$(0 \cdot 0) \oplus (1 \cdot 0) \oplus (1 \cdot 0) \oplus 1 = 1$	-1
001	$(0 \cdot 0) \oplus (1 \cdot 0) \oplus (1 \cdot 1) \oplus 1 = 0$	1
010	$(0 \cdot 0) \oplus (1 \cdot 1) \oplus (1 \cdot 0) \oplus 1 = 0$	1
011	$(0 \cdot 0) \oplus (1 \cdot 1) \oplus (1 \cdot 1) \oplus 1 = 1$	-1
100	$(0 \cdot 1) \oplus (1 \cdot 0) \oplus (1 \cdot 0) \oplus 1 = 1$	-1
101	$(0 \cdot 1) \oplus (1 \cdot 0) \oplus (1 \cdot 1) \oplus 1 = 0$	1
110	$(0 \cdot 1) \oplus (1 \cdot 1) \oplus (1 \cdot 0) \oplus 1 = 0$	1
111	$(0 \cdot 1) \oplus (1 \cdot 1) \oplus (1 \cdot 1) \oplus 1 = 1$	-1

Il termine $b = 1$ inverte tutti i valori della parità e tutti i segni. Confrontiamo lo stato dopo l'oracolo con quello ottenuto per $b = 0$.

$s = 011$, $b = 1$. Il termine costante b inverte i valori della funzione. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Funzione affine: una funzione lineare con un termine costante aggiunto tramite XOR.

La preparazione e i segni della funzione affine

Partiamo da 000 in A e da 1 nel bersaglio. La preparazione uniforme produce gli otto ingressi; i valori della tabella affine determinano poi il segno di ciascun termine.



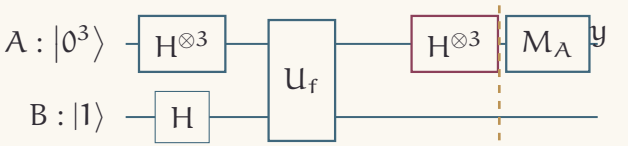
$$
\begin{aligned}
|\Psi_0\rangle &= |000\rangle\,|1\rangle\,,\\
|\Psi_1\rangle &= \tfrac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle\\
&\quad + |100\rangle + |101\rangle + |110\rangle + |111\rangle)\,|-\rangle\,,\\
|\Psi_2\rangle &= \tfrac{1}{\sqrt{8}}(-|000\rangle + |001\rangle + |010\rangle - |011\rangle\\
&\quad - |100\rangle + |101\rangle + |110\rangle - |111\rangle)\,|-\rangle\,,\\
(-1)^{s\cdot x\oplus 1} &= -(-1)^{s\cdot x}.
\end{aligned}
$$

Tutte le ampiezze sono moltiplicate per lo stesso segno meno. Le Hadamard sono lineari, quindi anche lo stato finale conserverà questo fattore comune. Svolgiamo le somme per verificare quale risultato rimane e come cambia la sua ampiezza.

Con $s = 011$ e $b = 1$, i segni sono $\sigma = (-1, 1, 1, -1, -1, 1, 1, -1)$ nell'ordine da 000 a 111. Ogni ampiezza vale $\sigma_x/\sqrt{8}$. Il registro B resta in $|-\rangle$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Funzione affine: una funzione lineare con un termine costante aggiunto tramite XOR. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Stringa 011, b=1: ampiezze 000 e 001

Iniziamo dalle uscite 000 e 001. Il vettore dei segni è $\sigma = (-1,1,1,-1,-1,1,1,-1)$: moltiplichiamo queste componenti per le righe corrispondenti della matrice di Hadamard, quindi sommiamo.



Dopo le Hadamard finali

$$\mathbf{r}_{000} = (1,1,1,1,1,1,1,1),$$
$$\sigma \odot \mathbf{r}_{000} = (-1,1,1,-1,-1,1,1,-1),$$
$$A_{000} = \frac{-1+1+1-1-1+1+1-1}{8} = 0.$$

Uscita $y = 000$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\mathbf{r}_{001} = (1,-1,1,-1,1,-1,1,-1),$$
$$\sigma \odot \mathbf{r}_{001} = (-1,-1,1,1,-1,-1,1,1),$$
$$A_{001} = \frac{-1-1+1+1-1-1+1+1}{8} = 0.$$

Uscita $y = 001$: contributi $\pm 1/8$



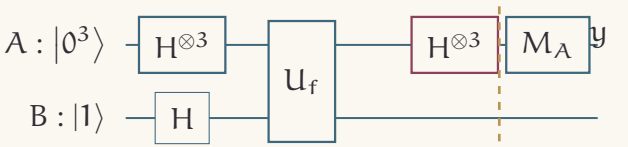
Somma delle ampiezze: 0

Le uscite 000 e 001 hanno ancora ampiezza zero. Il segno comune ha invertito ogni contributo e le cancellazioni restano valide. Controlliamo le componenti 010 e 011.

$\sigma = (-1,1,1,-1,-1,1,1,-1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 011, b=1: ampiezze 010 e 011

Le uscite fino a 001 sono già state calcolate. Proseguiamo con 010 e 011, conservando $\sigma = (-1,1,1,-1,-1,1,1,-1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\mathbf{r}_{010} = (1,1,-1,-1,1,1,-1,-1),$$
$$\sigma \odot \mathbf{r}_{010} = (-1,1,-1,1,-1,1,-1,1),$$
$$A_{010} = \frac{-1+1-1+1-1+1-1+1}{8} = 0.$$

Uscita $y = 010$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\mathbf{r}_{011} = (1,-1,-1,1,1,-1,-1,1),$$
$$\sigma \odot \mathbf{r}_{011} = (-1,-1,-1,-1,-1,-1,-1,-1),$$
$$A_{011} = \frac{-1-1-1-1-1-1-1-1}{8} = -1.$$

Uscita $y = 011$: contributi $\pm 1/8$



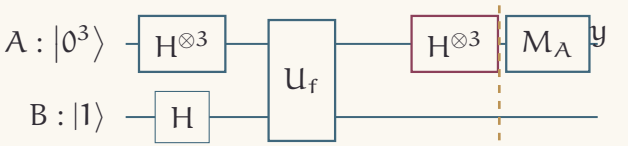
Somma delle ampiezze: -1

L'uscita 010 si annulla, mentre 011 ha ampiezza -1. Abbiamo quindi individuato il termine che può comparire in misura. Verifichiamo anche le quattro uscite residue prima di interpretare il segno meno.

$\sigma = (-1,1,1,-1,-1,1,1,-1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

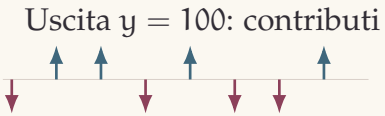
Stringa 011, b=1: ampiezze 100 e 101

Le uscite fino a 011 sono già state calcolate. Proseguiamo con 100 e 101, conservando $\sigma = (-1,1,1,-1,-1,1,1,-1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\begin{aligned} \mathbf{r}_{100} &= (1,1,1,1,-1,-1,-1,-1),\\ \sigma \odot \mathbf{r}_{100} &= (-1,1,1,-1,1,-1,-1,1),\\ A_{100} &= \frac{-1+1+1-1+1-1-1+1}{8} = 0. \end{aligned}$$



$$\begin{aligned} \mathbf{r}_{101} &= (1,-1,1,-1,-1,1,-1,1),\\ \sigma \odot \mathbf{r}_{101} &= (-1,-1,1,1,1,1,-1,-1),\\ A_{101} &= \frac{-1-1+1+1+1+1-1-1}{8} = 0. \end{aligned}$$

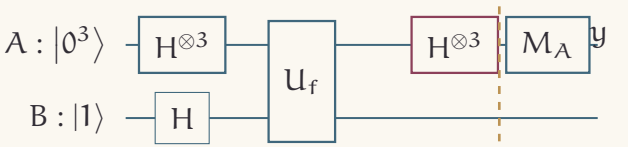


Le componenti 100 e 101 sono zero. Nessuna di queste due uscite aggiunge un possibile risultato della misura. Restano da controllare 110 e 111.

$\sigma = (-1,1,1,-1,-1,1,1,-1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Stringa 011, b=1: ampiezze 110 e 111

Le uscite fino a 101 sono già state calcolate. Proseguiamo con 110 e 111, conservando $\sigma = (-1,1,1,-1,-1,1,1,-1)$; ciascuna riga di Hadamard produce una nuova somma, divisa per 8.



Dopo le Hadamard finali

$$\begin{aligned} \mathbf{r}_{110} &= (1,1,-1,-1,-1,-1,1,1), \\ \sigma \odot \mathbf{r}_{110} &= (-1,1,-1,1,1,-1,1,-1), \\ A_{110} &= \frac{-1+1-1+1+1-1+1-1}{8} = 0. \end{aligned}$$

Uscita $y = 110$: contributi $\pm 1/8$



Somma delle ampiezze: 0

$$\begin{aligned} \mathbf{r}_{111} &= (1,-1,-1,1,-1,1,1,-1), \\ \sigma \odot \mathbf{r}_{111} &= (-1,-1,-1,-1,1,1,1,1), \\ A_{111} &= \frac{-1-1-1-1+1+1+1+1}{8} = 0. \end{aligned}$$

Uscita $y = 111$: contributi $\pm 1/8$



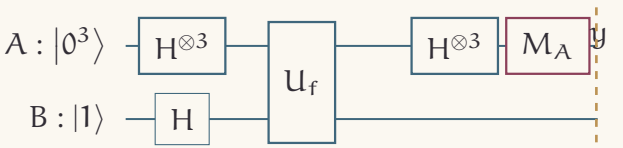
Somma delle ampiezze: 0

Anche le ultime due componenti si annullano. Il vettore finale ha una sola ampiezza non nulla, pari a -1 su 011. Calcoliamo il suo modulo quadro per vedere se questo segno distingue il valore di b.

$\sigma = (-1,1,1,-1,-1,1,1,-1)$ contiene i segni dopo l'oracolo. $\mathbf{r}_y$ è la riga dei segni di Hadamard per l'esito y. $\odot$ moltiplica componente per componente. Sommiamo i prodotti e dividiamo per 8. Ordine: da 000 a 111. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

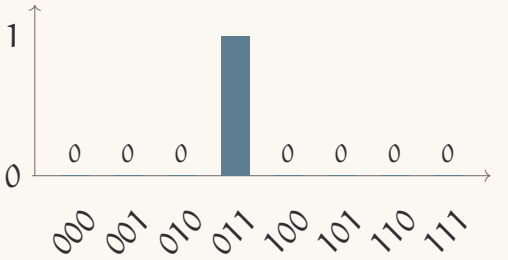
La fase globale e le probabilità

Le somme hanno lasciato il termine $-|011\rangle$. Per $b = 0$ avremmo ottenuto $|011\rangle$. La probabilità della misura dipende dal modulo quadro dell'ampiezza: calcoliamolo nei due casi.



Misura di A: risultato y

Probabilità per entrambi i valori di b



Risultato della misura in A

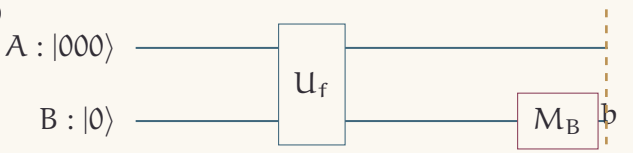
$$b = 0 : \ |\Psi_3\rangle = |011\rangle\,|-\rangle\,, \qquad b = 1 : \ |\Psi_3\rangle = -\,|011\rangle\,|-\rangle\,,$$
$$p(011) = |-1|^2 = (-1)(-1) = 1, \quad p(y \neq 011) = 0,$$
$$|(-1)A_y|^2 = (-1)^2|A_y|^2 = |A_y|^2.$$

Entrambi i valori di b danno probabilità uno al risultato 011. La misura ricostruisce quindi $s = 011$. Per determinare anche il termine costante interroghiamo ora la funzione sull'ingresso nullo.

Una fase globale moltiplica tutte le ampiezze per lo stesso fattore di modulo uno. Qui il fattore è $(-1)^b$. A_y indica una generica ampiezza dello stato. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La ricostruzione del termine costante

Abbiamo ricostruito $s = 011$ e dobbiamo ancora determinare b. Facciamo una nuova interrogazione preparando A in $|000\rangle$ e B in $|0\rangle$. Con tutti i bit di ingresso nulli, la parità vale zero e la risposta della funzione è proprio b.



Seconda interrogazione: misura di B

$$f_{s,b}(000) = s_2 \cdot 0 \oplus s_1 \cdot 0 \oplus s_0 \cdot 0 \oplus b = b,$$
$$f_{011,1}(000) = 0 \oplus 0 \oplus 0 \oplus 1 = 1,$$
$$U_f |000\rangle_A |0\rangle_B = |000\rangle_A |0 \oplus 1\rangle_B = |000\rangle_A |1\rangle_B .$$

Leggiamo 1 in B e ricostruiamo $b = 1$. Il procedimento quantistico ha usato una chiamata per s e una per b. Calcoliamo anche quante interrogazioni richiede la ricostruzione classica della stessa funzione affine.

0^n è l'ingresso con tutti i bit a zero, quindi $f(0^n) = b$. e_j ha un solo bit 1 nella posizione j. Poiché $f(e_j) = s_j \oplus b$, lo XOR con b restituisce s_j. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Funzione affine: una funzione lineare con un termine costante aggiunto tramite XOR. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La stessa funzione affine ricostruita classicamente

Interroghiamo prima 000 e otteniamo $b = 1$. Interroghiamo poi un ingresso con un solo bit uguale a uno. La risposta contiene il coefficiente di quella posizione e il termine costante. Facendo XOR con b eliminiamo il termine già noto.

$$f_{s,b}(e_j) = s_j \oplus b \quad \Longrightarrow \quad f_{s,b}(e_j) \oplus b = s_j \oplus \underbrace{b \oplus b}_{0} = s_j.$$

Ingresso	Risposta per $s = 011$, $b = 1$	Coefficiente ricavato
100	$0 \oplus 1 = 1$	$s_2 = 1 \oplus 1 = 0$
010	$1 \oplus 1 = 0$	$s_1 = 0 \oplus 1 = 1$
001	$1 \oplus 1 = 0$	$s_0 = 0 \oplus 1 = 1$

Una risposta determina b e altre tre determinano $s = 011$. Con n coefficienti questo metodo usa $n + 1$ interrogazioni. Torniamo ora alla famiglia lineare, in cui $b = 0$ è noto, e confrontiamo il numero di accessi necessari.

e_j è l'ingresso con un solo 1 nella posizione j. Lo XOR di un bit con se stesso vale zero: $b \oplus b = 0$. Funzione affine: una funzione lineare con un termine costante aggiunto tramite XOR.

Le interrogazioni classiche per n coefficienti

Torniamo alla famiglia lineare $f_s(x) = s \cdot x$, quindi poniamo $b = 0$. Il conteggio sarà n; per la famiglia affine con b ignoto serviva anche l'interrogazione nell'origine. La scelta degli ingressi con un solo bit attivo vale per qualunque lunghezza. Sostituiamo e_j nella definizione della funzione, separando la posizione j da tutte le altre.

$$(e_j)_k = \begin{cases} 1 & k = j, \\ 0 & k \neq j, \end{cases}$$

$$f_s(e_j) = \bigoplus_{k=0}^{n-1} s_k (e_j)_k = s_j \cdot 1 \oplus \bigoplus_{k \neq j} s_k \cdot 0 = s_j,$$

$$s = (f(e_{n-1}), \ldots, f(e_0)).$$

n coefficienti

↓

e_j isola s_j

↓

n interrogazioni sufficienti

Per la famiglia lineare bastano n interrogazioni, una per ogni coefficiente. Per capire se un metodo classico esatto possa usarne meno, contiamo quante stringhe nascoste deve riuscire a distinguere.

e_j è l'ingresso con un solo bit 1 nella posizione j. Nella famiglia $f_s(x) = s \cdot x$, la risposta $f_s(e_j) = s_j$ isola il coefficiente di quella posizione. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Funzione affine: una funzione lineare con un termine costante aggiunto tramite XOR.

Il limite informativo classico

Un algoritmo classico deterministico deve identificare ogni stringa senza errori. Anche se sceglie l'ingresso in funzione delle risposte precedenti, ogni risposta introduce al massimo due alternative nel percorso di esecuzione.

$$\begin{aligned} q \text{ risposte binarie} &\implies \text{al massimo } 2^q \text{ percorsi,} \\ \#\{s\} = 2^n, \quad 2^q \geq 2^n \quad &\implies \quad q \geq n. \end{aligned}$$

Una risposta: al massimo 2 rami

↓

Due risposte: al massimo 4 rami

↓

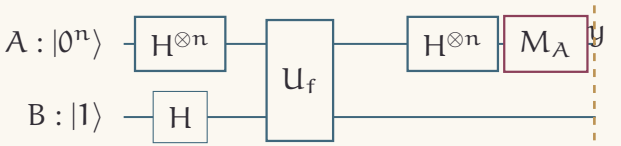
q risposte: al massimo 2^q rami

Le 2^n stringhe possibili richiedono almeno 2^n sequenze distinguibili di risposte. Poiché q risposte binarie offrono al più 2^q sequenze, occorre $q \geq n$. Il metodo che interroga i vettori della base raggiunge questo limite. Raccogliamo ora anche le risorse quantistiche.

Il conteggio assume un algoritmo classico deterministico, esatto per ogni s, con una risposta di un bit per interrogazione. n coefficienti indipendenti danno 2^n stringhe possibili.

Le risorse della ricostruzione

Il confronto riguarda anzitutto il numero di accessi alla funzione. Le porte esterne e la realizzazione interna dell'oracolo costituiscono costi distinti, che devono essere dichiarati per interpretare il vantaggio.



Risorsa	Classico esatto	Circuito BV
Interrogazioni	n	1
Hadamard esterne	—	$n + 1 + n = 2n + 1$
Qubit	—	$n + 1$
Bit misurati	—	n

In Bernstein–Vazirani la preparazione e le Hadamard finali trasformano i coefficienti della parità nella stringa misurata. Studiamo ora una funzione che nasconde s attraverso coppie di ingressi con la stessa uscita: dovremo capire quale informazione renda disponibile la sua misura.

A contiene n qubit e B un qubit. Se tutti partono da zero, una X prepara B in $|1\rangle$. I conteggi distinguono le chiamate all'oracolo dalle altre porte e dalla famiglia affine con termine costante. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. Oracolo: operazione che rende disponibile la funzione f.

Da Bernstein–Vazirani a Simon

Nel problema di Bernstein–Vazirani abbiamo cercato una stringa nascosta s. I suoi bit indicavano quali posizioni dell'ingresso partecipavano al calcolo della parità. Anche in Simon cerchiamo una stringa attraverso interrogazioni a una funzione. Questa volta gli ingressi sono organizzati in coppie: i due ingressi di ciascuna coppia producono la stessa uscita.

$$\text{Bernstein–Vazirani:} \quad f_s(x) = s \cdot x.$$

$$\text{Simon:} \quad x \longmapsto x \oplus s, \qquad f(x) = f(x \oplus s).$$

BV: posizioni della parità

↓

In entrambi cerchiamo s

↓

Simon: relazione fra ingressi

La stringa s indica quali bit cambiare in un ingresso per ottenere il suo compagno. Ogni coppia deve produrre la stessa uscita, e la medesima stringa deve funzionare per tutti gli ingressi. Precisiamo questa promessa e poi verifichiamola su una funzione a due bit.

x e s sono stringhe di n bit. In Simon $s \neq 0^n$: il compagno $x \oplus s$ deve essere distinto da x. Ogni valore assunto da f corrisponde esattamente a due ingressi. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

Perché una coppia permette di trovare la stringa

Disponiamo di un oracolo per $f : \{0,1\}^n \to \{0,1\}^m$. Ci viene garantito che ogni valore assunto da f corrisponde esattamente a due ingressi. Per ingressi distinti, $f(x) = f(z)$ se e solo se $z = x \oplus s$, con la stessa stringa $s \neq 0^n$. Questa è la promessa del problema. Trovata una coppia, ricaviamo s calcolando:

$$\begin{aligned} x \oplus z &= x \oplus (x \oplus s) \\ &= (x \oplus x) \oplus s \\ &= 0^n \oplus s \\ &= s. \end{aligned}$$

Due ingressi distinti

$$f(x) = f(z)$$

$$s = x \oplus z$$

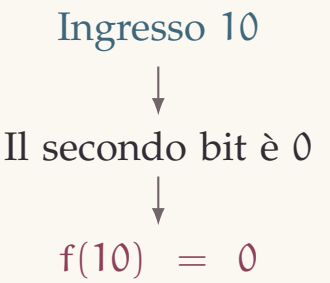
Lo XOR con s applicato due volte riporta all'ingresso iniziale, perché $s \oplus s = 0^n$. Gli ingressi si organizzano quindi in coppie. La promessa esclude $s = 0^n$, così i due membri di ogni coppia sono distinti. Scegliamo una funzione concreta e individuiamoli.

$s \neq 0^n$. Per $x \neq z$: $f(x) = f(z) \iff x \oplus z = s$. Lo XOR fra stringhe agisce separatamente su ciascuna posizione. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

Una funzione a due bit

Consideriamo un ingresso $x = x_1x_0$, formato da due bit. Scegliamo una funzione che restituisce il secondo: $f(x_1x_0) = x_0$. Per costruire la tabella leggiamo quindi il bit nella posizione x_0.

Ingresso x_1x_0	x_1	x_0	$f(x) = x_0$
00	0	0	0
01	0	1	1
10	1	0	0
11	1	1	1



La tabella mostra due coppie: $00, 10$ danno uscita zero e $01, 11$ danno uscita uno. Per ricostruire la stringa che le collega, calcoliamo quali bit cambiano passando da un ingresso al suo compagno.

Istanza: due bit in ingresso e un bit in uscita. La formula della funzione serve al lettore per verificare l'esempio; il risolutore conosce il formato dell'oracolo e la promessa di Simon.

Le coppie e il loro XOR

L'uscita zero compare per 00 e 10. L'uscita uno compare per 01 e 11. Calcoliamo lo XOR degli ingressi di ciascuna coppia, separatamente nelle due posizioni:

$$00 \oplus 10 = (0 \oplus 1,\ 0 \oplus 0) = (1, 0) = 10,$$
$$01 \oplus 11 = (0 \oplus 1,\ 1 \oplus 1) = (1, 0) = 10.$$
$$\boxed{s = 10}.$$



Entrambe le coppie hanno XOR uguale a 10. Questa verifica identifica la stringa dell'istanza. Ripartiamo ora dal punto di vista di chi riceve soltanto la scatola nera: deve scoprire s interrogando la funzione.

$0 \oplus 0 = 0, 0 \oplus 1 = 1, 1 \oplus 0 = 1, 1 \oplus 1 = 0$. La coppia $(1, 0)$ indica la stringa 10.

La prima interrogazione classica

Ripartiamo dal punto di vista del risolutore, che deve trovare s interrogando l'oracolo. La stringa ha due bit e la promessa esclude 00. All'inizio sono quindi possibili 01, 10 e 11. Scegliamo come primo ingresso 00 e registriamo la risposta:



$$s \in \{01, 10, 11\}.$$

$$f(00) = 0.$$

Archivio dopo il primo accesso: $(00, 0)$.

Le stringhe evidenziate soddisfano i vincoli acquisiti.

La prima risposta dice che $f(00) = 0$. Tutte e tre le stringhe $01, 10, 11$ possono ancora essere il compagno di 00 secondo una delle promesse possibili. Conserviamo la risposta e interroghiamo 01 per confrontare i due valori.

$s \neq 0^n$. Per $x \neq z$: $f(x) = f(z) \iff x \oplus z = s$. Lo XOR fra stringhe agisce separatamente su ciascuna posizione. Oracolo: operazione che rende disponibile la funzione f. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

La seconda interrogazione esclude un candidato

Interroghiamo 01 e riceviamo uno. Le risposte raccolte sono $f(00) = 0$ e $f(01) = 1$. Poiché sono diverse, 00 e 01 non formano una coppia. Il loro XOR è:

01 **10** **11**

$$00 \oplus 01 = (0 \oplus 0,\ 0 \oplus 1) = (0, 1) = 01,$$

$$f(00) \neq f(01) \implies s \neq 01.$$

$$\boxed{s \in \{10, 11\}}.$$

Le stringhe evidenziate soddisfano i vincoli acquisiti.

Con l'ipotesi $s = 01$, il compagno di 00 sarebbe 01 e le due risposte dovrebbero coincidere. Abbiamo osservato zero e uno, quindi questa ipotesi è esclusa. Restano 10 e 11. Interroghiamo 10 per distinguere le due possibilità.

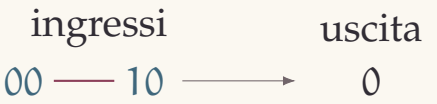
$s \neq 0^n$. Per $x \neq z$: $f(x) = f(z) \iff x \oplus z = s$. Lo XOR fra stringhe agisce separatamente su ciascuna posizione. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

La terza interrogazione individua una coppia

Interroghiamo ora 10. La risposta è zero, come per il primo ingresso. Le tre interrogazioni hanno prodotto:

Accesso	Ingresso	Risposta
1	00	0
2	01	1
3	10	0

$$f(00) = f(10) \implies s = 00 \oplus 10$$
$$= (0 \oplus 1,\ 0 \oplus 0) = (1, 0) = 10.$$

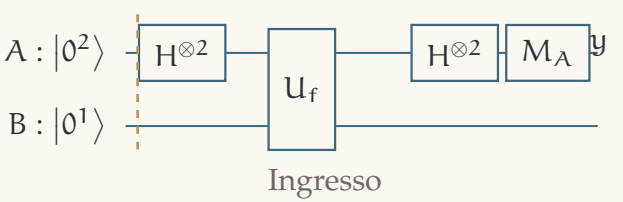


I due ingressi 00 e 10 hanno dato la stessa uscita. Il loro XOR è 10, che la promessa identifica con s. La ricerca classica ha richiesto tre interrogazioni. Manteniamo questa funzione e prepariamo il circuito quantistico.

$s \neq 0^n$. Per $x \neq z$: $f(x) = f(z) \iff x \oplus z = s$. Lo XOR fra stringhe agisce separatamente su ciascuna posizione. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

I registri e l'azione dell'oracolo

L'ingresso ha due bit, quindi usiamo due qubit nel registro A. L'uscita ha un solo bit, quindi basta un qubit nel registro B. Come in Bernstein–Vazirani, l'oracolo conserva l'ingresso e aggiorna il bersaglio mediante XOR:



$$U_f |x\rangle_A |t\rangle_B = |x\rangle_A |t \oplus f(x)\rangle_B .$$

$$0 \oplus 0 = 0, \quad 0 \oplus 1 = 1 \implies$$

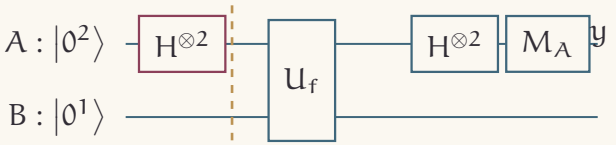
$$U_f |x\rangle_A |0\rangle_B = |x\rangle_A |f(x)\rangle_B .$$

In Bernstein–Vazirani preparavamo B in $|-\rangle$ per produrre i segni della funzione. Qui B parte da $|0\rangle$ e riceve direttamente $f(x)$. Potremo così raccogliere nello stesso ramo gli ingressi con uguale uscita. Seguiamo la preparazione dei tre qubit.

$U_f^2 |x, t\rangle = |x, t \oplus f(x) \oplus f(x)\rangle = |x, t\rangle$: due applicazioni ripristinano il bersaglio. Nell'istanza $f(x) = x_0$, una CNOT da x_0 a B realizza l'oracolo. Qubit: sistema con stati di base $|0\rangle, |1\rangle$. Registro: gruppo di qubit. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. CNOT: inverte il bit bersaglio quando il bit di controllo vale 1. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x. Nel circuito, M_A misura A e M_B misura B. La linea oro indica il punto raggiunto.

La sovrapposizione degli ingressi

Partiamo con A, il registro dei due bit di ingresso, in $|00\rangle_A$ e B, il registro dell'uscita, in $|0\rangle_B$. Applichiamo una Hadamard a ciascun qubit di A. Il registro B resta zero:



Dopo le prime Hadamard

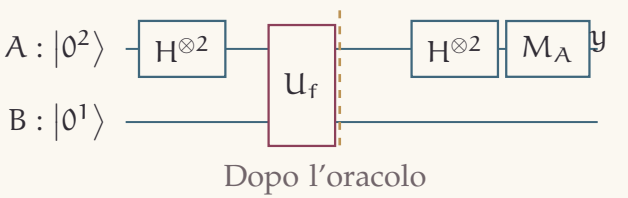
$$
\begin{aligned}
|\Psi_{\text{prep}}\rangle &= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes |0\rangle_B \\
&= \frac{1}{2}\big(|0\rangle\,|0\rangle + |0\rangle\,|1\rangle + |1\rangle\,|0\rangle + |1\rangle\,|1\rangle\big)\,|0\rangle_B \\
&= \frac{1}{2}\big(|00\rangle + |01\rangle + |10\rangle + |11\rangle\big)_A\,|0\rangle_B\,.
\end{aligned}
$$

A contiene tutti i quattro ingressi con ampiezza 1/2. B è ancora nello stato $|0\rangle$. Applicando l'oracolo, ogni termine conserverà il proprio ingresso in A e registrerà il valore della funzione in B.

Istanza: $n = 2$, $m = 1$, $f(x_1x_0) = x_0$, $s = 10$. $|x,t\rangle = |x\rangle_A \otimes |t\rangle_B$. Le stringhe sono ordinate come x_1x_0. La norma quadrata è $4 \cdot |1/2|^2 = 4 \cdot 1/4 = 1$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Sovrapposizione: somma di stati, ciascuno pesato dalla propria ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'oracolo sui quattro termini

Per la funzione scelta, $f(x_1x_0) = x_0$. Applichiamo la regola a ciascun termine della sovrapposizione. Nella scrittura $|x, t\rangle$, la virgola separa i due registri:



Dopo l'oracolo

$$
\begin{aligned}
U_f\,|00,0\rangle &= |00,0\oplus 0\rangle = |00,0\rangle\,,\\
U_f\,|01,0\rangle &= |01,0\oplus 1\rangle = |01,1\rangle\,,\\
U_f\,|10,0\rangle &= |10,0\oplus 0\rangle = |10,0\rangle\,,\\
U_f\,|11,0\rangle &= |11,0\oplus 1\rangle = |11,1\rangle\,.
\end{aligned}
$$

ingressi	uscita
00 — 10	0
01 — 11	1

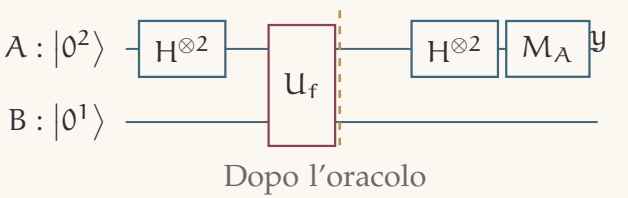
$$|\Psi_{\text{oracolo}}\rangle = \frac{1}{2}\big(|00,0\rangle + |01,1\rangle + |10,0\rangle + |11,1\rangle\big).$$

La funzione vale zero per 00, 10 e uno per 01, 11. Questi valori sono ora scritti in B. Per capire come usarli, distinguiamo il ruolo dell'ingresso conservato in A da quello dell'uscita registrata in B.

Istanza: $n = 2$, $m = 1$, $f(x_1x_0) = x_0$, $s = 10$. $|x, t\rangle = |x\rangle_A \otimes |t\rangle_B$. Le stringhe sono ordinate come x_1x_0. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Sovrapposizione: somma di stati, ciascuno pesato dalla propria ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Che cosa contengono adesso A e B

Dopo l'oracolo, A contiene ancora l'ingresso e B contiene il valore della funzione. La virgola separa i due registri. Leggiamo prima un singolo termine, poi lo stato completo:



$$|10,0\rangle = \underbrace{|10\rangle_A}_{\text{ingresso } 10} \underbrace{|0\rangle_B}_{f(10)=0}.$$

Stato dopo l'oracolo:

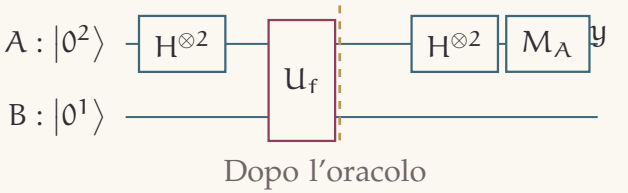
$$\frac{1}{2}\left(|00\rangle_A|0\rangle_B + |01\rangle_A|1\rangle_B + |10\rangle_A|0\rangle_B + |11\rangle_A|1\rangle_B\right).$$

La stessa uscita di B accompagna due ingressi diversi. La relazione cercata è proprio lo XOR fra questi ingressi. Riordiniamo quindi lo stato raccogliendo insieme i termini che hanno lo stesso valore di B.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A|t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Perché raggruppiamo i termini con la stessa uscita

Vogliamo vedere che cosa accadrebbe misurando soltanto B, il registro che contiene $f(x)$. Riordiniamo i termini e raccogliamo i fattori uguali di B. In questo passaggio cambiamo soltanto la scrittura dello stato:



Dopo l'oracolo

$$\frac{1}{2}\left(|00\rangle_A|0\rangle_B + |10\rangle_A|0\rangle_B + |01\rangle_A|1\rangle_B + |11\rangle_A|1\rangle_B\right)$$

$$= \frac{1}{2}\underbrace{\left(|00\rangle + |10\rangle\right)_A|0\rangle_B}_{\text{termini compatibili con B=0}}$$

$$+ \frac{1}{2}\underbrace{\left(|01\rangle + |11\rangle\right)_A|1\rangle_B}_{\text{termini compatibili con B=1}} .$$

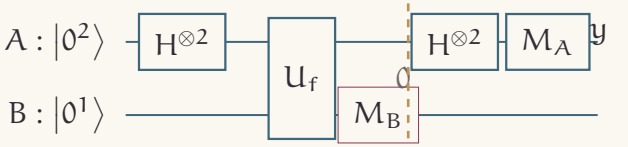
ingressi	uscita
00 — 10 →	0
01 — 11 →	1

Le due parentesi mostrano le coppie associate alle uscite zero e uno. Seguiamo prima B uguale a zero fino alle probabilità della misura di A. Ripeteremo il conto per B uguale a uno, poi useremo l'esito di A per ricavare la stringa nascosta.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A|t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Leggiamo B e supponiamo di ottenere zero

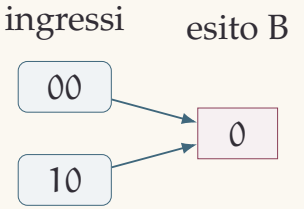
L'esito zero della lettura di B è compatibile con due termini dello stato congiunto. Questi termini hanno entrambi ampiezza 1/2. Per calcolare la probabilità dell'esito sommiamo i loro moduli quadri:



Lettura di B: coppia selezionata

Termini selezionati: $\frac{1}{2}|00\rangle_A|0\rangle_B + \frac{1}{2}|10\rangle_A|0\rangle_B$,

$$P(B=0) = \left|\frac{1}{2}\right|^2 + \left|\frac{1}{2}\right|^2 = \frac{1}{4}+\frac{1}{4} = \frac{1}{2}.$$



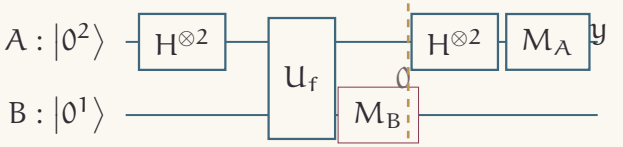
L'esito di B seleziona la coppia di ingressi.

La lettura B uguale a zero lascia compatibili entrambi gli ingressi 00 e 10. Il vettore selezionato ha norma quadrata 1/2, pari alla probabilità del ramo. Per descrivere lo stato dopo la misura dobbiamo riportare questa norma a uno.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A|t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Norma: radice della somma dei moduli quadri dei coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Dopo la selezione, le probabilità devono sommare a uno

Sappiamo ormai che B vale zero. Lo stato di A deve quindi assegnare probabilità totale uno ai due ingressi rimasti. Dividiamo il vettore selezionato per la radice della probabilità dell'esito, cioè per $\sqrt{1/2} = 1/\sqrt{2}$:



Lettura di B: coppia selezionata

$$\text{Stato di A dopo B} = 0: \quad \frac{(|00\rangle + |10\rangle)/2}{1/\sqrt{2}}$$

$$= \frac{\sqrt{2}}{2}(|00\rangle + |10\rangle) = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

$$\text{Controllo:} \quad \left|\frac{1}{\sqrt{2}}\right|^2 + \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2} + \frac{1}{2} = 1.$$

Dividendo per $1/\sqrt{2}$, ciascuna ampiezza diventa $1/\sqrt{2}$ e i due moduli quadri sommano a uno. B resta in $|0\rangle$ e A conserva la sovrapposizione dei due ingressi. Valutiamo che cosa accadrebbe leggendo A subito.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x, t\rangle = |x\rangle_A |t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Sovrapposizione: somma di stati, ciascuno pesato dalla propria ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

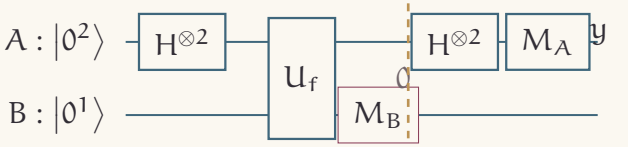
Perché misurare direttamente la coppia non basta

Il registro A è ora nello stato $(|00\rangle + |10\rangle)/\sqrt{2}$. Se lo misurassimo subito, otterremmo un solo ingresso della coppia. Vediamo esattamente quali risultati sarebbero possibili:

$$|\phi_{B=0}\rangle = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

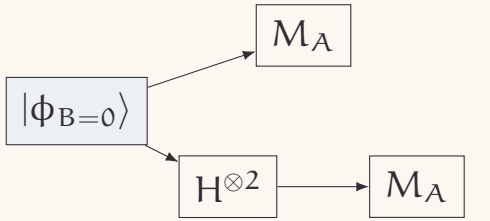
$$P(A = 00 \mid B = 0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2},$$

$$P(A = 10 \mid B = 0) = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}.$$



Coppia selezionata: prima delle H finali

Confronto ipotetico



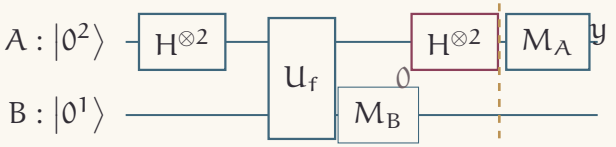
Procedimento con interferenza

Una misura immediata sceglierebbe uno dei due ingressi della coppia. Per estrarre invece informazione sulla relazione che li lega, applichiamo le Hadamard ad A: le loro trasformate potranno sommarsi o cancellarsi per ciascun risultato finale.

Istanza: $n = 2$, $m = 1$, $f(x_1x_0) = x_0$, $s = 10$. $|x, t\rangle = |x\rangle_A \otimes |t\rangle_B$. Le stringhe sono ordinate come x_1x_0. Questo confronto ipotetico con la misura diretta non aggiunge una misura al circuito di Simon. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard trasformano il termine 00

Lo stato normalizzato di A è $(|00\rangle + |10\rangle)/\sqrt{2}$. Per linearità possiamo trasformare un termine alla volta e sommare i risultati. Cominciamo da $|00\rangle$: ognuno dei suoi due qubit usa $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$.



Dopo le Hadamard finali

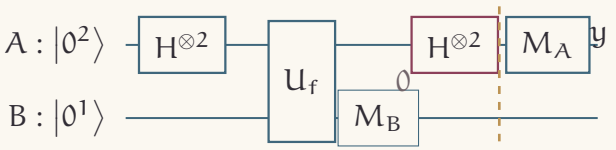
$$
\begin{aligned}
H^{\otimes 2}|00\rangle &= (H|0\rangle) \otimes (H|0\rangle) \\
&= \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle) \\
&= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).
\end{aligned}
$$

I quattro termini hanno coefficiente $1/2$, prodotto di due fattori $1/\sqrt{2}$. Il contributo di questa trasformata allo stato completo dovrà essere moltiplicato anche per il peso iniziale $1/\sqrt{2}$ della coppia. Calcoliamo prima la trasformata di $|10\rangle$.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. La probabilità di un esito è il modulo quadro della sua ampiezza. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Linearità: si trasforma ogni termine dello stato e si sommano i risultati con gli stessi coefficienti. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard trasformano il termine 10

Nel secondo termine, il primo qubit vale uno. Per questo $H|1\rangle$ introduce un segno meno davanti a $|1\rangle$. Il secondo qubit vale zero e si trasforma come prima:



Dopo le Hadamard finali

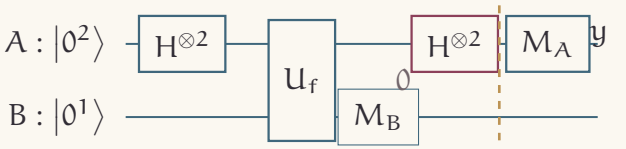
$$
\begin{aligned}
H^{\otimes 2}|10\rangle &= (H|1\rangle) \otimes (H|0\rangle) \\
&= \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\
&= \frac{1}{2}(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle - |1\rangle|1\rangle) \\
&= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle).
\end{aligned}
$$

Per i risultati 00 e 01 entrambe le trasformate hanno segno positivo. Per 10 e 11 la seconda ha segno negativo. Mettiamo ora accanto i contributi allo stesso risultato e sommiamoli, includendo il peso della coppia.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. La probabilità di un esito è il modulo quadro della sua ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le uscite 10 e 11 si cancellano

La lettura B = 0 ha lasciato A nello stato $(|00\rangle + |10\rangle)/\sqrt{2}$. Sommiamo le due trasformate appena scritte, con il fattore comune $(1/\sqrt{2})(1/2) = 1/(2\sqrt{2})$.



Dopo le Hadamard finali

$$H^{\otimes 2}\frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\Big[(1+1)\,|00\rangle + (1+1)\,|01\rangle + (1-1)\,|10\rangle + (1-1)\,|11\rangle\Big]$$

$$= \frac{2\,|00\rangle + 2\,|01\rangle}{2\sqrt{2}} = \frac{|00\rangle + |01\rangle}{\sqrt{2}}.$$

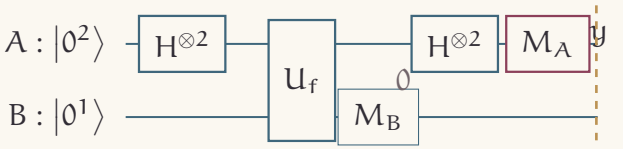
I contributi rossi a $|10\rangle$ e $|11\rangle$ si cancellano. Quelli blu a $|00\rangle$ e $|01\rangle$ sommano a 2. Dividendo per $2\sqrt{2}$, le ampiezze rimaste valgono $1/\sqrt{2}$. Calcoliamo le probabilità della misura.

Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La misura restituisce 00 oppure 01

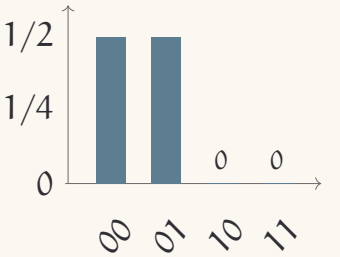
La somma ha lasciato lo stato $(|00\rangle + |01\rangle)/\sqrt{2}$. Il coefficiente di ciascun termine rimasto vale $1/\sqrt{2}$. La regola di Born assegna a ogni risultato il modulo quadro della sua ampiezza:

Esito di A: y	Ampiezza	Probabilità, dato B = 0
00	$1/\sqrt{2}$	$\lvert 1/\sqrt{2}\rvert^2 = 1/2$
01	$1/\sqrt{2}$	$\lvert 1/\sqrt{2}\rvert^2 = 1/2$
10	0	0
11	0	0



Misura di A: risultato y

Probabilità di A, dato B=0



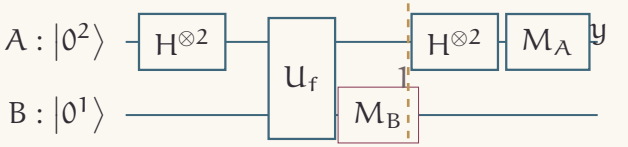
Risultato della misura in A

Queste probabilità descrivono il ramo selezionato da B uguale a zero. Per completare la distribuzione di A dobbiamo esaminare anche l'altra coppia. Ripartiamo dallo stato dopo l'oracolo e seguiamo la lettura B uguale a uno.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A |t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Se B dà uno, cambia la coppia selezionata

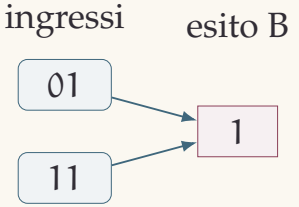
Torniamo allo stato dopo l'oracolo. Questa volta la lettura di B, il registro di $f(x)$, dà uno. Restano i termini con ingressi 01 e 11. Calcoliamo la probabilità dell'esito e normalizziamo lo stato di A:



Lettura di B: coppia selezionata

$$P(B = 1) = |1/2|^2 + |1/2|^2 = 1/2,$$

$$\text{Stato di A dopo } B = 1: \quad \frac{(|01\rangle + |11\rangle)/2}{\sqrt{1/2}} = \frac{|01\rangle + |11\rangle}{\sqrt{2}}.$$



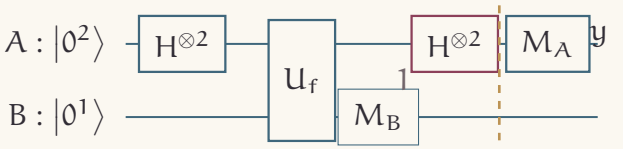
L'esito di B seleziona la coppia di ingressi.

La seconda lettura seleziona 01, 11, ancora con XOR uguale a 10. Ogni ingresso ha di nuovo ampiezza $1/\sqrt{2}$ nello stato normalizzato. Applichiamo le Hadamard e confrontiamo il risultato con quello della prima coppia.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x, t\rangle = |x\rangle_A |t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La seconda coppia cambia un segno finale

Per B = 1, A è nello stato $\frac{|01\rangle+|11\rangle}{\sqrt{2}}$. Sviluppiamo i due ket e sommiamo, con il fattore comune $(1/\sqrt{2})(1/2) = 1/(2\sqrt{2})$.



Dopo le Hadamard finali

$$H^{\otimes 2}|01\rangle = \frac{1}{2}\Big[\,|00\rangle\ -|01\rangle\ +|10\rangle\ -|11\rangle\,\Big],$$

$$H^{\otimes 2}|11\rangle = \frac{1}{2}\Big[\,|00\rangle\ -|01\rangle\ -|10\rangle\ +|11\rangle\,\Big].$$

$$H^{\otimes 2}\frac{|01\rangle+|11\rangle}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\Big[\,(1+1)\,|00\rangle + (-1-1)\,|01\rangle + (1-1)\,|10\rangle + (-1+1)\,|11\rangle\,\Big]$$

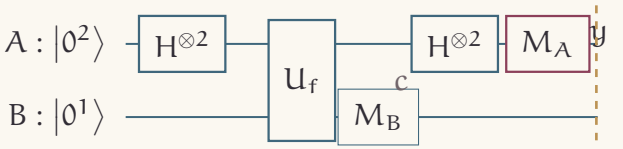
$$= \frac{2\,|00\rangle - 2\,|01\rangle}{2\sqrt{2}} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}.$$

Si cancellano i ket 10, 11. Restano i ket 00, 01, con ampiezza di modulo $1/\sqrt{2}$ e probabilità $|\pm 1/\sqrt{2}|^2 = 1/2$ ciascuno. Confrontiamo le due possibili letture di B.

Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma +2 oppure −2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

I due esiti di B portano alle stesse informazioni

Indichiamo con $p(y \mid B = c)$ la probabilità di leggere y in A sapendo che B ha dato c. Per entrambi i valori di B gli esiti finali sono 00 e 01, ciascuno con probabilità 1/2. Se non distinguiamo i due casi, pesiamo ciascuno con la probabilità 1/2:



Misura di A: risultato y

$$\begin{aligned} p(01) &= P(B=0)\,p(01 \mid B=0) + P(B=1)\,p(01 \mid B=1) \\ &= \tfrac{1}{2}\cdot\tfrac{1}{2} + \tfrac{1}{2}\cdot\tfrac{1}{2} = \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2}, \\ p(00) &= \tfrac{1}{2}, \qquad p(10) = p(11) = 0. \end{aligned}$$

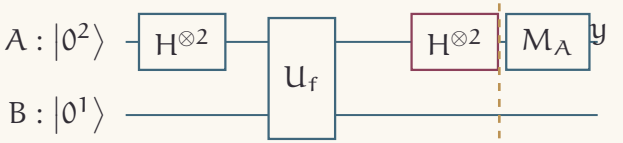
ingressi	uscita
00 — 10	0
01 — 11	1

La media dei due rami conserva probabilità 1/2 per 00 e 1/2 per 01. Abbiamo ottenuto la distribuzione complessiva di A. Verifichiamo ora che si possa ottenere la stessa distribuzione lasciando B senza misura intermedia.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A\,|t\rangle_B$. y: esito finale di A; s: stringa da ricostruire.

Lasciamo B senza misura e trasformiamo soltanto A

Ripartiamo dallo stato dopo l'oracolo, con entrambe le coppie presenti. Le Hadamard agiscono su A e lasciano B invariato. Usiamo le trasformazioni delle due somme di ingressi appena calcolate:



Dopo le Hadamard finali

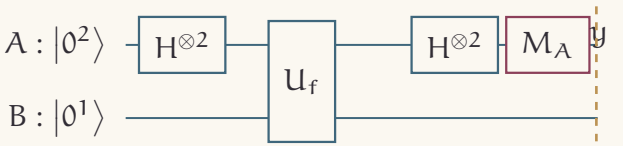
$$\begin{aligned}
\text{Prima:}\quad & \tfrac{1}{2}\big[(|00\rangle + |10\rangle)_A\,|0\rangle_B + (|01\rangle + |11\rangle)_A\,|1\rangle_B\big], \\
\text{Dopo:}\quad & \tfrac{1}{2}\big[(|00\rangle + |01\rangle)_A\,|0\rangle_B + (|00\rangle - |01\rangle)_A\,|1\rangle_B\big] \\
& = \tfrac{1}{2}\big(|00,0\rangle + |01,0\rangle + |00,1\rangle - |01,1\rangle\big).
\end{aligned}$$

Lo stato finale contiene quattro termini del sistema A e B. Il risultato A uguale a 01 compare con due valori diversi di B. Per calcolarne la probabilità sommiamo i moduli quadri delle due ampiezze, come vediamo nel conto seguente.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A\,|t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La probabilità finale non richiede la lettura di B

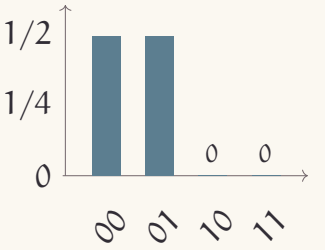
Lo stato congiunto finale è $(|00,0\rangle + |01,0\rangle + |00,1\rangle - |01,1\rangle)/2$. I termini con B diverso sono stati di base distinti. Se misuriamo soltanto A, sommiamo le loro probabilità:



Misura di A: risultato y

$$
\begin{aligned}
p(A = 01) &= p(A = 01, B = 0) + p(A = 01, B = 1) \\
&= \left|\tfrac{1}{2}\right|^2 + \left|-\tfrac{1}{2}\right|^2 = \tfrac{1}{2}, \\
p(A = 00) &= \left|\tfrac{1}{2}\right|^2 + \left|\tfrac{1}{2}\right|^2 = \tfrac{1}{2}, \\
p(A = 10) &= p(A = 11) = 0.
\end{aligned}
$$

Stesse probabilità senza misurare B



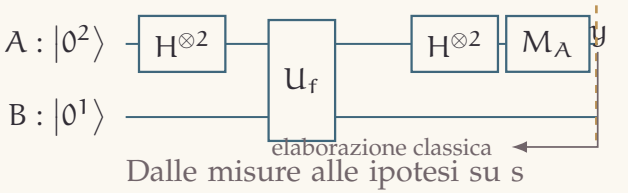
Risultato della misura in A

Ritroviamo la stessa distribuzione di A: 00 e 01 sono equiprobabili anche lasciando B senza misura. Dobbiamo ancora ricavare la stringa nascosta. Supponiamo di aver letto 01 e confrontiamo le tre ipotesi possibili su s.

A: due qubit per l'ingresso; B: un qubit per $f(x) = x_0$. $|x,t\rangle = |x\rangle_A |t\rangle_B$. y: esito finale di A; s: stringa da ricostruire. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Quale stringa nascosta permette il risultato A = 01?

Dopo la misura $A = 01$, confrontiamo $s = 01, 10, 11$. Per ogni ingresso, moltiplichiamo l'ampiezza iniziale $1/2$ per il coefficiente di Hadamard. Sommiamo le ampiezze con lo stesso B, poi i loro moduli quadri.



$$\text{Ingressi } 00, 10: \quad (1/2)\cdot(1/2) = +1/4, \qquad \text{ingressi } 01, 11: \quad (1/2)\cdot(-1/2) = -1/4.$$

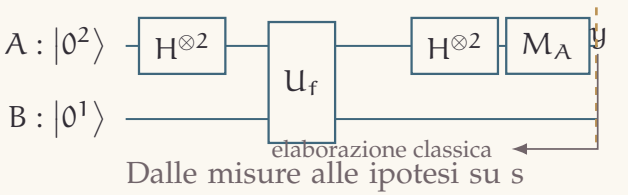
Stringa ipotizzata	Ingressi → uscita della scatola nera	Ampiezze finali con $A = 01$	Probabilità di misurare $A = 01$
$s = 01$	$00, 01 \mapsto 0$ $10, 11 \mapsto 1$	$B = 0: \quad 1/4 - 1/4 = 0$ $B = 1: \quad 1/4 - 1/4 = 0$	$0^2 + 0^2 = 0$
$s = 10$	$00, 10 \mapsto 0$ $01, 11 \mapsto 1$	$B = 0: \quad 1/4 + 1/4 = 1/2$ $B = 1: \quad -1/4 - 1/4 = -1/2$	$(1/2)^2 + (-1/2)^2 = 1/2$
$s = 11$	$00, 11 \mapsto 0$ $01, 10 \mapsto 1$	$B = 0: \quad 1/4 - 1/4 = 0$ $B = 1: \quad -1/4 + 1/4 = 0$	$0^2 + 0^2 = 0$

Solo $s = 10$ rende possibile la misura 01: abbiamo ricostruito la stringa. Esaminiamo adesso l'esito 00.

B parte da $|0\rangle$. Le uscite di B sono etichette intercambiabili. La promessa esclude $s = 00$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

La misura 00 lascia aperte tutte le ipotesi

La distribuzione dell'esempio permette anche il risultato A uguale a 00. Per questo termine finale, le Hadamard danno coefficiente $+1/2$ da ciascun ingresso. Moltiplicando per l'ampiezza iniziale $1/2$, ogni contributo vale $+1/4$, qualunque sia la coppia.



$$\text{Ogni coppia:} \qquad \frac{1}{4} + \frac{1}{4} = \frac{1}{2}.$$

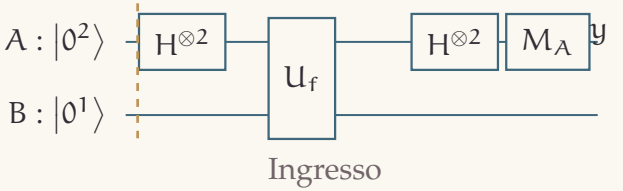
Ipotesi su s	Ampiezza con B = 0	Ampiezza con B = 1	P(A = 00)
01	1/2	1/2	$(1/2)^2 + (1/2)^2 = 1/2$
10	1/2	1/2	$(1/2)^2 + (1/2)^2 = 1/2$
11	1/2	1/2	$(1/2)^2 + (1/2)^2 = 1/2$

La misura 00 è compatibile con tutte e tre le stringhe nascoste. Prepariamo di nuovo i registri e ripetiamo il circuito. Nell'istanza studiata, il risultato 01 permette di concludere $s = 10$. Verifichiamo adesso lo stesso procedimento su una funzione con coppie diverse.

00 è qui un risultato misurato in A. La promessa esclude invece la stringa nascosta $s = 00$. Le ampiezze in tabella appartengono allo stato congiunto, con B lasciato senza misura. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Una nuova scatola nera: cambia la coppia di ingressi

Scegliamo una nuova funzione a due bit: $f(x_1x_0) = x_1 \oplus x_0$. Il circuito mantiene la stessa preparazione e le stesse porte esterne. Cambiano le risposte della scatola nera e quindi le coppie che dovremo riconoscere.



x	$f(x)$
00	$0 \oplus 0 = 0$
01	$0 \oplus 1 = 1$
10	$1 \oplus 0 = 1$
11	$1 \oplus 1 = 0$

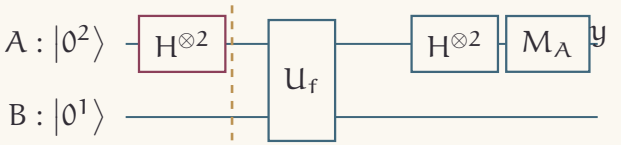


Gli ingressi 00, 11 danno zero e 01, 10 danno uno. Le due coppie hanno lo stesso XOR: $00 \oplus 11 = 01 \oplus 10 = 11$. Il lettore può verificare la stringa dell'istanza. Seguiamo il circuito per vedere come la ricostruisce dalle misure.

x_1 è il primo bit dell'ingresso, x_0 il secondo. $f(x_1x_0) = x_1 \oplus x_0$. La stringa nascosta è lo XOR dei due ingressi con la stessa uscita. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

La preparazione nell'istanza 11

Prepariamo A in $|00\rangle$ e B in $|0\rangle$, come nel primo esempio. Le Hadamard agiscono soltanto su A. Sviluppiamo il prodotto tensoriale per ottenere i quattro ingressi su cui applicheremo la nuova funzione.



Dopo le prime Hadamard

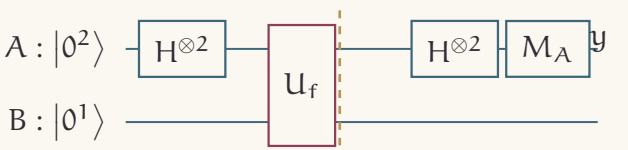
$$|\Psi_{\text{inizio}}\rangle = |00\rangle\,|0\rangle\,,$$
$$|\Psi_{\text{prep}}\rangle = \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \tfrac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle$$
$$= \tfrac{1}{2}(|00,0\rangle + |01,0\rangle + |10,0\rangle + |11,0\rangle).$$

Ogni ingresso ha ampiezza 1/2 e B è ancora zero. Sostituiamo ora i valori della nuova funzione per vedere quali ingressi condividono la stessa etichetta.

A contiene due qubit di ingresso; B parte da $|0\rangle$. Dopo la preparazione, ciascuno dei quattro ingressi ha ampiezza 1/2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Prodotto tensoriale: combina stati di registri distinti e moltiplica le rispettive ampiezze. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le nuove coppie dopo l'oracolo

La preparazione uniforme è la stessa del primo esempio. Ora l'oracolo registra $x_1 \oplus x_0$. Sostituiamo i quattro valori nel bersaglio inizialmente zero, poi raccogliamo i termini con la stessa uscita:



Dopo l'oracolo

$$
\begin{aligned}
|\Psi_{\text{oracolo}}\rangle &= \tfrac{1}{2}\big(|00, 0 \oplus 0\rangle + |01, 0 \oplus 1\rangle \\
&\qquad + |10, 0 \oplus 1\rangle + |11, 0 \oplus 0\rangle\big) \\
&= \tfrac{1}{2}(|00, 0\rangle + |01, 1\rangle + |10, 1\rangle + |11, 0\rangle) \\
&= \tfrac{1}{2}(|00\rangle + |11\rangle)\,|0\rangle + \tfrac{1}{2}(|01\rangle + |10\rangle)\,|1\rangle\,.
\end{aligned}
$$

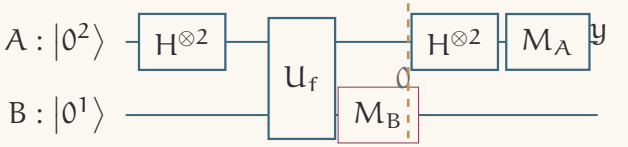
ingressi	uscita
00 — 11	0
01 — 10	1

B uguale a zero seleziona la coppia 00, 11; B uguale a uno seleziona 01, 10. Seguiamo prima la lettura zero. Per applicare le Hadamard allo stato selezionato dobbiamo calcolarne la probabilità e normalizzarlo.

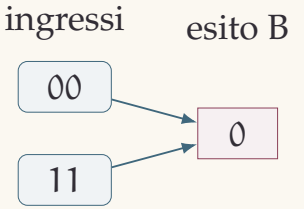
$|x, c\rangle = |x\rangle_A\,|c\rangle_B$: x è l'ingresso, $c = f(x)$ l'uscita della scatola nera. Qui $f(x_1x_0) = x_1 \oplus x_0$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

B uguale a zero seleziona ora 00 e 11

La funzione è ora $f(x_1x_0) = x_1 \oplus x_0$. A contiene due bit di ingresso e B un bit di uscita. Se leggiamo zero in B, sopravvivono i termini $|00,0\rangle/2$ e $|11,0\rangle/2$. Normalizziamo A:



Lettura di B: coppia selezionata



L'esito di B seleziona la coppia di ingressi.

$$\text{Stato di A:} \quad \frac{(|00\rangle + |11\rangle)/2}{\sqrt{1/2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

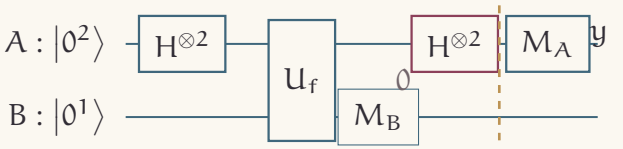
$$P(B = 0) = \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2},$$

La divisione per $\sqrt{1/2}$ restituisce ampiezza $1/\sqrt{2}$ a ciascun ingresso. Lo stato di A è ora $(|00\rangle + |11\rangle)/\sqrt{2}$. Calcoliamo le due trasformate e sommiamo i contributi allo stesso risultato finale.

Leggere $B = 0$ seleziona la coppia di ingressi $00, 11$. Dividere per $\sqrt{P(B = 0)}$ rende unitaria la norma dello stato di A. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

L'interferenza della coppia 00 e 11

Per $B = 0$, A è nello stato $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Sviluppiamo i due ket e sommiamo, con il fattore comune $(1/\sqrt{2})(1/2) = 1/(2\sqrt{2})$.



Dopo le Hadamard finali

$$H^{\otimes 2}|00\rangle = \frac{1}{2}\Big[\,|00\rangle\ +|01\rangle\ +|10\rangle\ +|11\rangle\,\Big],$$

$$H^{\otimes 2}|11\rangle = \frac{1}{2}\Big[\,|00\rangle\ -|01\rangle\ -|10\rangle\ +|11\rangle\,\Big].$$

$$H^{\otimes 2}\frac{|00\rangle+|11\rangle}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\Big[\,(1+1)\,|00\rangle + (1-1)\,|01\rangle + (1-1)\,|10\rangle + (1+1)\,|11\rangle\,\Big]$$

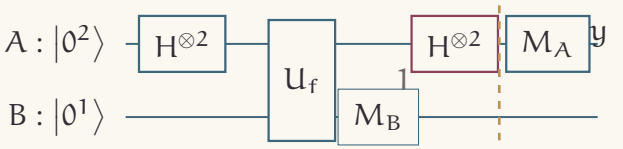
$$= \frac{2\,|00\rangle + 2\,|11\rangle}{2\sqrt{2}} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}.$$

Si cancellano i ket 01, 10. Restano i ket 00, 11, con ampiezza di modulo $1/\sqrt{2}$ e probabilità $|\pm 1/\sqrt{2}|^2 = 1/2$ ciascuno. Seguiamo adesso anche la lettura B = 1.

Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La coppia alternativa conferma gli stessi esiti

Per $B = 1$, A è nello stato $\frac{|01\rangle+|10\rangle}{\sqrt{2}}$. Sviluppiamo i due ket e sommiamo, con il fattore comune $(1/\sqrt{2})(1/2) = 1/(2\sqrt{2})$.



Dopo le Hadamard finali

$$H^{\otimes 2}|01\rangle = \frac{1}{2}\Big[\,|00\rangle\ -|01\rangle\ +|10\rangle\ -|11\rangle\,\Big],$$

$$H^{\otimes 2}|10\rangle = \frac{1}{2}\Big[\,|00\rangle\ +|01\rangle\ -|10\rangle\ -|11\rangle\,\Big].$$

$$H^{\otimes 2}\frac{|01\rangle+|10\rangle}{\sqrt{2}} = \frac{1}{2\sqrt{2}}\Big[\,(1+1)\,|00\rangle + (-1+1)\,|01\rangle + (1-1)\,|10\rangle + (-1-1)\,|11\rangle\,\Big]$$

$$= \frac{2\,|00\rangle - 2\,|11\rangle}{2\sqrt{2}} = \frac{|00\rangle - |11\rangle}{\sqrt{2}}.$$

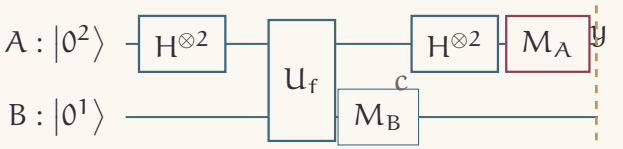
Si cancellano i ket 01, 10. Restano i ket 00, 11, con ampiezza di modulo $1/\sqrt{2}$ e probabilità $|\pm 1/\sqrt{2}|^2 = 1/2$ ciascuno. Possiamo ora riunire le probabilità dei due casi.

Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La misura di A può dare 00 oppure 11

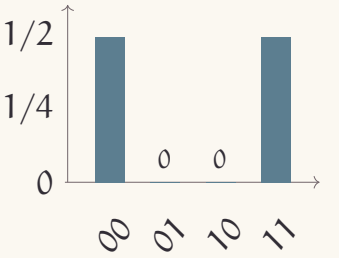
Per entrambi gli esiti di B, la probabilità finale di 00 e di 11 è 1/2. Sommiamo i contributi dei due casi, ciascuno pesato con la probabilità 1/2 della lettura di B:

$$
\begin{aligned}
p(00) &= \tfrac{1}{2}\tfrac{1}{2} + \tfrac{1}{2}\tfrac{1}{2} = \tfrac{1}{4} + \tfrac{1}{4} = \tfrac{1}{2},\\
p(01) &= \tfrac{1}{2}\cdot 0 + \tfrac{1}{2}\cdot 0 = 0,\\
p(10) &= \tfrac{1}{2}\cdot 0 + \tfrac{1}{2}\cdot 0 = 0,\\
p(11) &= \tfrac{1}{2}\tfrac{1}{2} + \tfrac{1}{2}\tfrac{1}{2} = \tfrac{1}{2}.
\end{aligned}
$$



Misura di A: risultato y

Probabilità del registro A



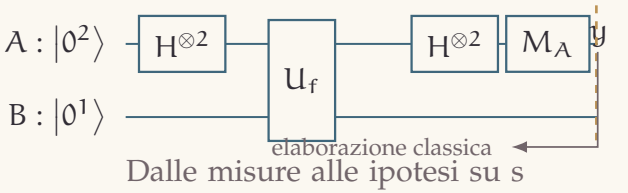
Risultato della misura in A

La distribuzione complessiva assegna probabilità 1/2 a 00 e a 11. Se osserviamo 11, quali stringhe nascoste restano compatibili? Ripetiamo il confronto fra le coppie previste dalle tre ipotesi.

I due valori di B selezionano coppie diverse. Per ciascuna, le probabilità di A sono $p(00) = p(11) = 1/2$ e $p(01) = p(10) = 0$.

Quale stringa nascosta permette il risultato A = 11?

Abbiamo misurato $A = 11$. Ogni ingresso $00, 01, 10, 11$ entra nella scatola nera con ampiezza $1/2$. B parte da $|0\rangle$ e riceve l'uscita $f(x)$. Ogni contributo finale è il prodotto dell'ampiezza iniziale per il coefficiente delle Hadamard.



$$\text{Ingressi } 00, 11: \quad (1/2)\cdot(1/2) = +1/4, \qquad \text{ingressi } 01, 10: \quad (1/2)\cdot(-1/2) = -1/4.$$

Sommiamo i contributi con lo stesso B, poi i moduli quadri delle due ampiezze ottenute.

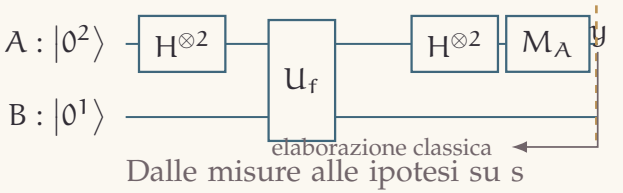
Stringa ipotizzata	Ingressi → uscita della scatola nera	Ampiezze finali con $A = 11$	Probabilità di misurare $A = 11$
$s = 01$	$00, 01 \mapsto 0$ $10, 11 \mapsto 1$	$B = 0$: $1/4 - 1/4 = 0$ $B = 1$: $-1/4 + 1/4 = 0$	$0^2 + 0^2 = 0$
$s = 10$	$00, 10 \mapsto 0$ $01, 11 \mapsto 1$	$B = 0$: $1/4 - 1/4 = 0$ $B = 1$: $-1/4 + 1/4 = 0$	$0^2 + 0^2 = 0$
$s = 11$	$00, 11 \mapsto 0$ $01, 10 \mapsto 1$	$B = 0$: $1/4 + 1/4 = 1/2$ $B = 1$: $-1/4 - 1/4 = -1/2$	$(1/2)^2 + (-1/2)^2 = 1/2$

Solo $s = 11$ rende possibile la misura 11. Una nuova esecuzione serve quando A dà invece 00.

Le uscite di B sono etichette intercambiabili. La promessa esclude $s = 00$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

Le esecuzioni proseguono fino a un risultato utile

Consideriamo ancora la funzione $f(x_1x_0) = x_1 \oplus x_0$. Ogni esecuzione produce 00 oppure 11, ciascuno con probabilità 1/2. Dopo ogni misura prepariamo nuovamente A e B nello stato iniziale. Una possibile sequenza è:



Esecuzione	Risultato misurato in A	Stringhe nascoste compatibili
1	00	01, 10, 11
2	00	01, 10, 11
3	11	11

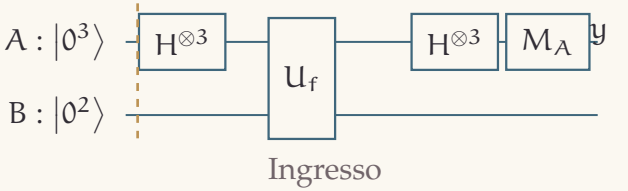
$$P(00, 00, 11) = \frac{1}{2} \cdot \frac{1}{2} \cdot \frac{1}{2} = \frac{1}{8}.$$

Le prime due misure lasciano invariato l'elenco. La terza identifica $s = 11$ e conclude la ricerca. Nei casi a due bit è bastato un risultato non nullo. Passiamo a tre bit: vedremo una misura non nulla lasciare ancora più candidate.

Ogni esecuzione usa una chiamata all'oracolo e una nuova preparazione dei registri. La sequenza mostrata è una delle possibili sequenze di risultati. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Con tre bit, una misura può lasciare più candidati

Nei casi a due bit un risultato non nullo ha identificato la stringa nascosta. Con tre bit le ipotesi iniziali sono sette. Seguiamo una funzione concreta per vedere come le misure restringono progressivamente l'elenco e quali risultati lasciano invariata l'informazione.



Stringhe nascoste possibili: 001, 010, 011, 100, 101, 110, 111.

$$f(x_2x_1x_0) = (x_1,\ x_2 \oplus x_0).$$

Il primo bit dell'uscita copia il bit centrale dell'ingresso; il secondo è lo XOR del primo e dell'ultimo bit. Il registro A contiene tre qubit e B ne contiene due.

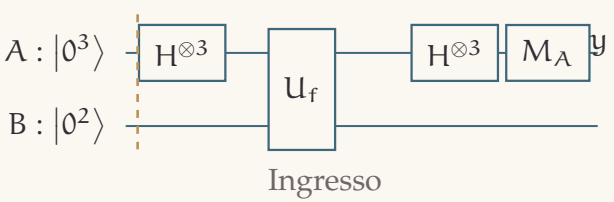
Scriviamo la funzione per controllare ogni passaggio dell'esempio. Il procedimento di ricerca dispone della scatola nera e della promessa sulle coppie; deve ricostruire la stringa nascosta dalle misure.

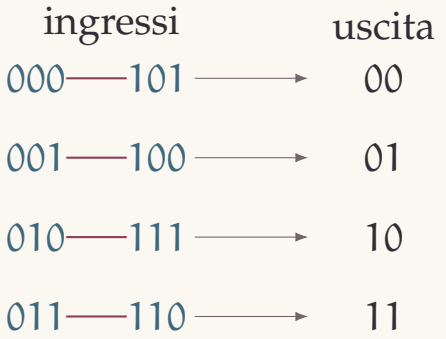
x_2: primo bit; x_1: bit centrale; x_0: ultimo bit. La promessa esclude la stringa nascosta 000. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

La funzione dell'esempio a tre bit

Per ogni ingresso calcoliamo le due componenti: il bit x_1 e la parità di x_2 e x_0. La tabella fornisce i valori da sostituire nello stato dopo l'oracolo.

x	$f(x)$
000	$(0, 0 \oplus 0) = 00$
001	$(0, 0 \oplus 1) = 01$
010	$(1, 0 \oplus 0) = 10$
011	$(1, 0 \oplus 1) = 11$
100	$(0, 1 \oplus 0) = 01$
101	$(0, 1 \oplus 1) = 00$
110	$(1, 1 \oplus 0) = 11$
111	$(1, 1 \oplus 1) = 10$



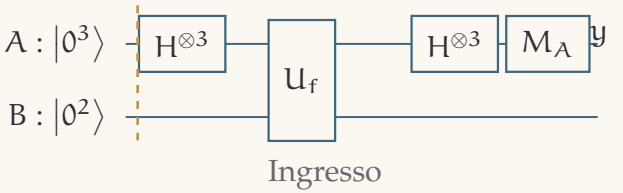


Le uscite uguali individuano quattro coppie. Verifichiamo con lo XOR che tutte abbiano la stessa stringa nascosta.

Ingresso: $x_2x_1x_0$. Uscita in B: $(x_1, x_2 \oplus x_0)$. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f.

Le uscite della scatola nera identificano quattro coppie

Verifichiamo tutte le coppie della tabella. Lo XOR viene calcolato posizione per posizione; la coincidenza della stringa risultante certifica la proprietà richiesta nell'istanza scelta.



$$
\begin{aligned}
000 \oplus 101 &= (0\oplus 1, 0\oplus 0, 0\oplus 1) = 101,\\
001 \oplus 100 &= (0\oplus 1, 0\oplus 0, 1\oplus 0) = 101,\\
010 \oplus 111 &= (0\oplus 1, 1\oplus 1, 0\oplus 1) = 101,\\
011 \oplus 110 &= (0\oplus 1, 1\oplus 1, 1\oplus 0) = 101.
\end{aligned}
$$

ingressi	uscita
000 — 101	00
001 — 100	01
010 — 111	10
011 — 110	11

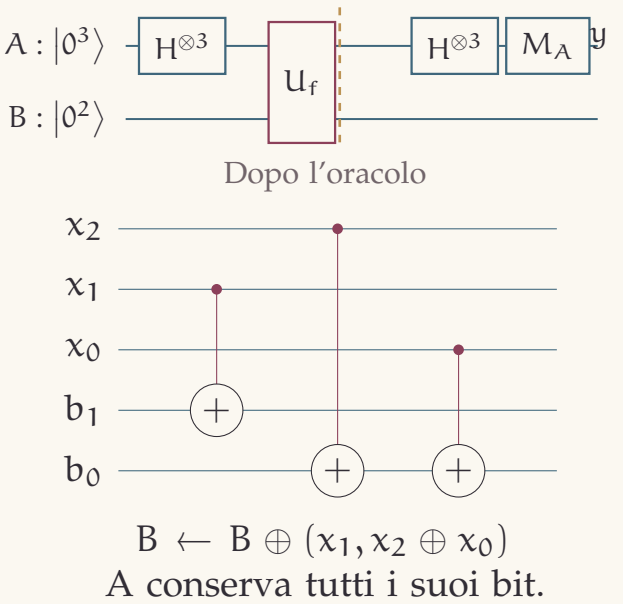
Le quattro coppie hanno tutte XOR uguale a 101 e le loro uscite sono distinte. La funzione soddisfa quindi la promessa con questa stringa. Mostriamo una realizzazione reversibile dell'oracolo prima di applicarlo ai registri quantistici.

Il lettore può verificare dalla tabella che lo XOR degli ingressi di ogni coppia è 101. Il circuito non riceve questa stringa come dato. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$. Reversibile: dall'uscita completa si può ricostruire l'ingresso.

Le porte dell'oracolo nell'istanza 101

Per verificare materialmente $f(x_2x_1x_0) = (x_1, x_2 \oplus x_0)$ usiamo tre CNOT. Indichiamo con b_1b_0 il contenuto di B: il primo bit riceve x_1, il secondo riceve prima x_2 e poi x_0, sempre mediante XOR.

$$
\begin{aligned}
&b_1 \leftarrow b_1 \oplus x_1, \quad b_0 \leftarrow b_0 \oplus x_2, \quad b_0 \leftarrow b_0 \oplus x_0,\\
&x = 110,\ B = 00: \quad 00 \longrightarrow 10 \longrightarrow 11 \longrightarrow 11,\\
&\qquad\qquad f(110) = (1, 1 \oplus 0) = 11,\\
&x = 110,\ B = 11: \quad 11 \longrightarrow 01 \longrightarrow 00 \longrightarrow 00.
\end{aligned}
$$

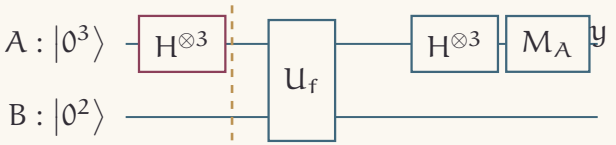


Applicare due volte l'oracolo ripristina B: questo conto ne verifica la reversibilità. Ogni esecuzione di Simon userà una sola chiamata. La costruzione lineare è visibile al lettore per controllare l'esempio; il procedimento di ricerca usa la sola promessa sulle coppie. Prepariamo ora i cinque qubit.

B parte da $|00\rangle$. Una CNOT inverte il bit bersaglio se il bit di controllo vale 1; l'oracolo realizza $f(x_2x_1x_0) = (x_1, x_2 \oplus x_0)$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$. Reversibile: dall'uscita completa si può ricostruire l'ingresso.

Prepariamo i tre qubit di A e i due di B

Il circuito usa tre qubit in A e due in B. Prepariamo B in 00 ed espandiamo la sovrapposizione di A prima di applicare l'oracolo.



Dopo le prime Hadamard

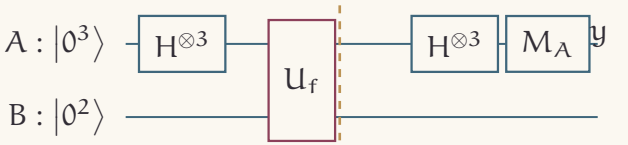
$$|\Psi_{\text{inizio}}\rangle = |000\rangle_A |00\rangle_B ,$$
$$|\Psi_{\text{prep}}\rangle = \frac{(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)(|0\rangle+|1\rangle)}{\sqrt{8}} |00\rangle$$
$$= \frac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle$$
$$+ |100\rangle + |101\rangle + |110\rangle + |111\rangle) |00\rangle .$$

I tre qubit di A generano otto ingressi con ampiezza $1/\sqrt{8}$. I due qubit di B sono zero e riceveranno le due componenti di $f(x)$. Applichiamo l'oracolo e raccogliamo i termini con la stessa uscita.

Tre Hadamard preparano gli otto ingressi di A con ampiezza $1/\sqrt{8}$; i due qubit di B restano nello stato $|00\rangle$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Sovrapposizione: somma di stati, ciascuno pesato dalla propria ampiezza. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Lo stato congiunto dell'istanza 101

Applichiamo la scatola nera a ciascun ingresso: B parte da 00 e riceve il valore della funzione. Poi raccogliamo i termini con la stessa uscita di B, perché possono contribuire insieme allo stesso risultato finale di A.



Dopo l'oracolo

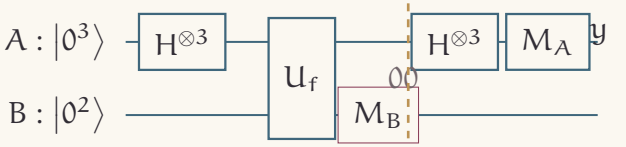
$$
\begin{aligned}
U_f\,|x, 00\rangle &= |x, f(x)\rangle\,, \\
|\Psi\rangle &= \tfrac{1}{\sqrt{8}}(|000, 00\rangle + |001, 01\rangle + |010, 10\rangle + |011, 11\rangle \\
&\qquad + |100, 01\rangle + |101, 00\rangle + |110, 11\rangle + |111, 10\rangle) \\
&= \tfrac{1}{\sqrt{8}}\big[(|000\rangle + |101\rangle)\,|00\rangle + (|001\rangle + |100\rangle)\,|01\rangle \\
&\qquad + (|010\rangle + |111\rangle)\,|10\rangle + (|011\rangle + |110\rangle)\,|11\rangle\big].
\end{aligned}
$$

Ogni etichetta di B compare accanto a due ingressi. Seguiamo prima la lettura $B = 00$, che seleziona 000 e 101. Calcoliamo la probabilità del ramo e lo stato normalizzato da trasformare con le Hadamard.

In $|x, c\rangle$, i primi tre bit appartengono ad A e gli ultimi due a B. Ogni termine congiunto ha ampiezza $1/\sqrt{8}$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=00 seleziona 000 e 101

In questa istanza A contiene tre qubit di ingresso e B due qubit di uscita. Supponiamo di leggere 00 in B. I termini compatibili hanno ingressi 000 e 101, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità e normalizziamo A:

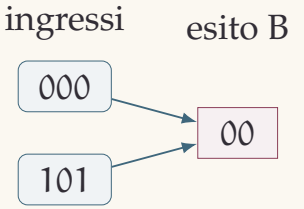


Lettura di B: coppia selezionata

$$P(B=00) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B=00)} = \frac{1}{2},$$

$$|\phi_{B=00}\rangle = \frac{(|000\rangle + |101\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|000\rangle + |101\rangle)$$

$$= \frac{|000\rangle + |101\rangle}{\sqrt{2}}.$$



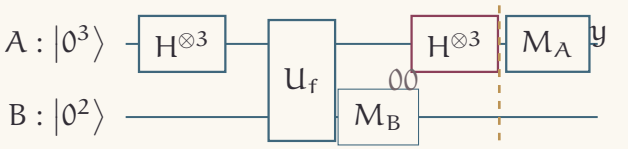
L'esito di B seleziona la coppia di ingressi.

Lo stato di A è ora $(|000\rangle + |101\rangle)/\sqrt{2}$. Applichiamo le Hadamard prima a $|000\rangle$, poi a $|101\rangle$. Sommeremo le due espansioni per vedere quali termini si cancellano.

L'uscita $B = 00$ ha probabilità $2/8 = 1/4$. Dopo averla selezionata, i due ingressi di A hanno ampiezza $1/\sqrt{2}$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 000 e 101

Dopo la lettura B = 00, A è nello stato $\frac{|000\rangle+|101\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\Big],$$

$$H^{\otimes 3}|101\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\Big].$$

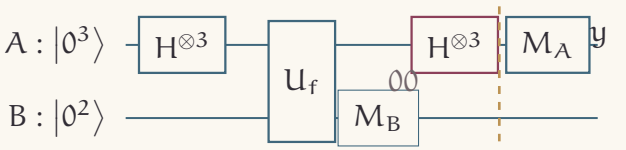
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 000 e 101

Sommiamo le due espansioni di $\frac{|000\rangle+|101\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|000\rangle + |101\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\left[\begin{array}{cccc} (1+1)|000\rangle & + (1-1)|001\rangle & + (1+1)|010\rangle & + (1-1)|011\rangle \\ + (1-1)|100\rangle & + (1+1)|101\rangle & + (1-1)|110\rangle & + (1+1)|111\rangle \end{array}\right]$$

$$= \frac{2|000\rangle + 2|010\rangle + 2|101\rangle + 2|111\rangle}{4} = \frac{|000\rangle + |010\rangle + |101\rangle + |111\rangle}{2}.$$

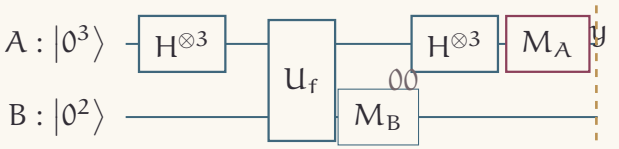
Ogni ampiezza rimasta vale 1/2. Calcoliamo le probabilità della misura.

A è il registro che misureremo. Qui B ha dato 00. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma +2 oppure −2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

I quattro risultati possibili della misura di A

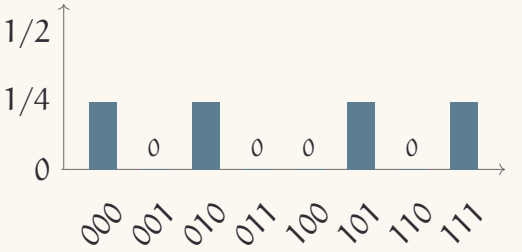
La somma delle due trasformate ha lasciato quattro termini, tutti con ampiezza 1/2. Misuriamo il registro A: la probabilità di ciascun risultato è il modulo quadro della sua ampiezza.

$$|\phi_{\text{finale}}\rangle = \frac{|000\rangle + |010\rangle + |101\rangle + |111\rangle}{2}.$$



Misura di A: risultato y

Probabilità di A, dato B=00



Risultato della misura in A

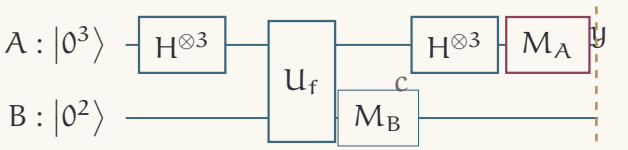
$$P(A = 000 \mid B = 00) = |1/2|^2 = 1/4,$$
$$P(A = 010 \mid B = 00) = |1/2|^2 = 1/4,$$
$$P(A = 101 \mid B = 00) = |1/2|^2 = 1/4,$$
$$P(A = 111 \mid B = 00) = |1/2|^2 = 1/4.$$
$$\tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} + \tfrac{1}{4} = 1.$$
$$P(A = 001) = P(A = 011) = P(A = 100) = P(A = 110) = 0.$$

Le uscite 000, 010, 101 e 111 hanno probabilità 1/4 ciascuna. Le altre quattro hanno probabilità zero. Confrontiamo ora le altre coppie selezionate da B.

Qui B=00 e $s = 101$. $P(A = y \mid B = 00)$ è la probabilità di y dopo questa lettura di B. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le quattro coppie dell'esempio 101

Le quattro uscite di B hanno ciascuna probabilità 1/4. Per ogni coppia normalizzata, la tabella riporta le ampiezze finali sui risultati di A indicati in colonna. Le altre quattro ampiezze sono zero.



Misura di A: risultato y

Uscita di B	Ingressi selezionati	A = 000 ampiezza	A = 010 ampiezza	A = 101 ampiezza	A = 111 ampiezza
00	000, 101	+1/2	+1/2	+1/2	+1/2
01	001, 100	+1/2	+1/2	−1/2	−1/2
10	010, 111	+1/2	−1/2	+1/2	−1/2
11	011, 110	+1/2	−1/2	−1/2	+1/2

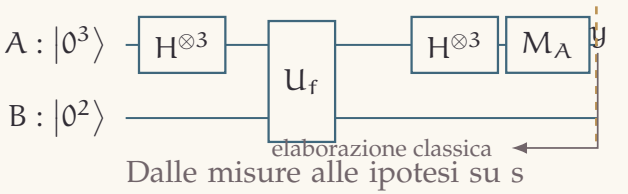
$$P(A = y) = 4 \cdot \underbrace{\tfrac{1}{4}}_{\text{probabilità di B}} \cdot \underbrace{(\tfrac{1}{2})^2}_{\text{probabilità di A dato B}} = \tfrac{1}{4}.$$

Ogni riga ha quattro ampiezze di modulo 1/2, quindi quattro risultati con probabilità 1/4. Usiamo le misure di A per restringere le ipotesi su s.

Conti completi: slide 160–168. Ogni riga descrive una coppia selezionata. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

Prima esecuzione: il risultato 000 non elimina ipotesi

Supponiamo di leggere A = 000. Per produrre questo termine finale, ogni Hadamard contribuisce con il segno più, qualunque sia il bit di ingresso. I due contributi di qualsiasi coppia si sommano.



$$\text{Qualunque coppia:} \quad \frac{(+1)(+1)(+1)+(+1)(+1)(+1)}{4} = \frac{1}{2}, \quad p(000) = \frac{1}{4}.$$

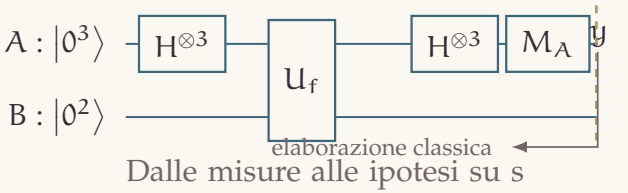
$$\text{Stringhe nascoste ancora possibili:} \quad 001,\ 010,\ 011,\ 100,\ 101,\ 110,\ 111.$$

Tutte e sette le ipotesi assegnano probabilità 1/4 al risultato 000. Questa prima esecuzione lascia quindi invariato l'elenco delle candidate. Prepariamo di nuovo i registri ed eseguiamo il circuito per ottenere un'altra misura.

A = 000 è il risultato della misura dopo le Hadamard. La stringa nascosta s descrive invece quali bit cambiano fra due ingressi con la stessa uscita.

La misura 010 esclude le stringhe con bit centrale 1

Nella seconda esecuzione leggiamo A = 010. Riprendiamo il calcolo in ciascuna coppia normalizzata. Per questo risultato conta solo il bit centrale dell'ingresso: se vale 0 il contributo è $+1/4$, se vale 1 è $-1/4$. Sommiamo i contributi dei due ingressi.



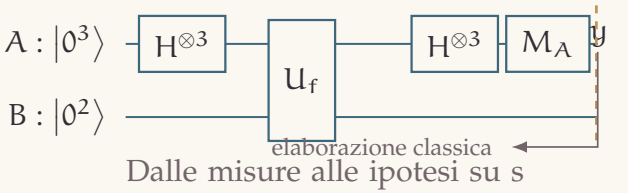
Stringhe nascoste ipotizzate	Bit centrale della stringa	Bit centrali dei due ingressi della coppia	Ampiezza nella coppia normalizzata per A = 010
010, 011, 110, 111	1	Diversi	$\frac{1}{4} - \frac{1}{4} = 0$
001, 100, 101	0	Uguali	$\pm(\frac{1}{4} + \frac{1}{4}) = \pm\frac{1}{2}$

Quando il bit centrale di s vale uno, i contributi si cancellano in ogni coppia e 010 sarebbe impossibile. La misura esclude quindi 010, 011, 110, 111. Restano 001, 100, 101, tutte con bit centrale zero. Una nuova esecuzione dovrà distinguere queste tre possibilità.

In una coppia normalizzata, $(1/\sqrt{2})(1/\sqrt{8}) = 1/4$. Il segno $\pm$ è quello dell'ampiezza del singolo risultato: $|+1/2|^2 = |-1/2|^2 = 1/4$. Un bit 1 di s indica una posizione che cambia fra i due ingressi. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

Un’altra misura 010 non distingue i tre candidati

Prepariamo di nuovo i registri ed eseguiamo il circuito una terza volta. Leggiamo ancora 010 in A. Tutte le tre stringhe rimaste prevedono questo risultato con la stessa probabilità, quindi il confronto conserva lo stesso elenco.



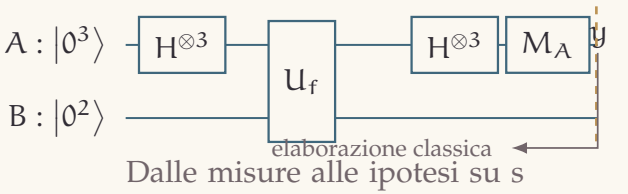
Stringa nascosta ipotizzata	Bit centrale	Compatibile con A = 010?
001	0	Sì
100	0	Sì
101	0	Sì

La sequenza osservata è 000, 010, 010. Le candidate restano 001, 100, 101. La terza prova ha ripetuto la condizione già ottenuta nella seconda. Eseguiamo di nuovo il circuito per cercare una condizione diversa.

Il numero di esecuzioni non coincide con il numero di informazioni diverse raccolte. Ogni esecuzione riparte dai registri inizializzati a zero.

La misura 111 lascia soltanto la stringa nascosta 101

Nella quarta esecuzione leggiamo A = 111. Sommiamo ancora i due contributi della coppia normalizzata. Ora tutte e tre le posizioni contano: cambiare un bit dell'ingresso inverte il segno, cambiarne due lo conserva. Confrontiamo i tre candidati rimasti.



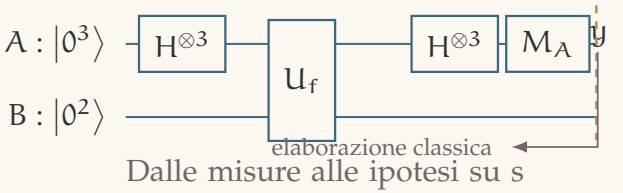
Stringa nascosta ipotizzata	Posizioni che cambiano fra i due ingressi	Ampiezza nella coppia normalizzata per A = 111	Compatibile con la misura?
001	Solo l'ultima	$\frac{1}{4} - \frac{1}{4} = 0$	No
100	Solo la prima	$\frac{1}{4} - \frac{1}{4} = 0$	No
101	La prima e l'ultima	$\pm(\frac{1}{4} + \frac{1}{4}) = \pm\frac{1}{2}$	Sì

Le ipotesi 001 e 100 renderebbero impossibile 111 in ogni coppia. Rimane soltanto $s = 101$, compatibile sia con 010 sia con 111. Abbiamo ricostruito la stringa. Riscriviamo ora le stesse esclusioni come condizioni sui suoi singoli bit.

I due ingressi di una coppia hanno la stessa uscita della funzione. Nello stato normalizzato ciascuno pesa $1/\sqrt{2}$: dopo le tre Hadamard, ogni contributo vale $\pm(1/\sqrt{2})(1/\sqrt{8}) = \pm 1/4$. Qui la misura è 111 e la stringa ricostruita è 101. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

Gli stessi conti diventano due equazioni sui bit di s

Abbiamo già trovato la risposta confrontando le ipotesi. Scriviamo ora lo stesso ragionamento in forma compatta: s_2 è il primo bit nascosto, s_1 quello centrale e s_0 l'ultimo.



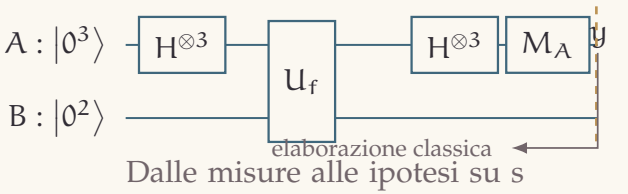
$$\begin{aligned}
\text{Misura A} = 010: &\quad s_1 = 0,\\
\text{Misura A} = 111: &\quad s_2 \oplus s_1 \oplus s_0 = 0 \quad \text{(un numero pari di cambi).}\\
\text{Sostituiamo } s_1 = 0: &\quad s_2 \oplus 0 \oplus s_0 = 0 \quad \Longrightarrow \quad s_2 = s_0.\\
(s_2, s_1, s_0) = (0,0,0) \text{ oppure } (1,0,1). &\qquad s \neq 000 \quad \Longrightarrow \quad \boxed{s = 101}.
\end{aligned}$$

Le due equazioni esprimono le cancellazioni già verificate. Per conservarle e combinarle quando aumentano i bit, possiamo raccoglierne i coefficienti in una matrice. Costruiamola usando proprio le misure 010 e 111.

Lo XOR vale 0 quando i due bit sono uguali: $0 \oplus 0 = 0$, $1 \oplus 1 = 0$. La promessa esclude la soluzione $s = 000$.

La matrice raccoglie le due condizioni già trovate

Ogni riga contiene i coefficienti di una condizione; le colonne corrispondono al primo bit s_2, al centrale s_1 e all'ultimo s_0. Sostituiamo la seconda riga con lo XOR delle due righe.



$$\underbrace{\begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}}_{\text{misure } 010,\ 111} \begin{pmatrix} s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \xrightarrow{R_2 \leftarrow R_2 \oplus R_1} \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

$$010 \oplus 111 = 101,$$

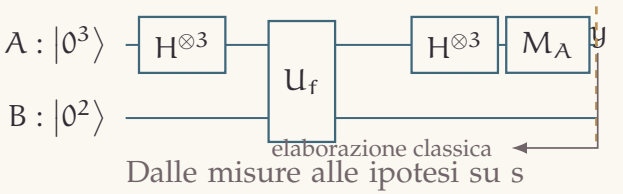
$$s_1 = 0, \quad s_2 \oplus s_0 = 0 \implies s \in \{000, 101\} \implies \boxed{s = 101}.$$

La nuova seconda riga esprime $s_2 \oplus s_0 = 0$, ottenuta usando $s_1 = 0$. Lo XOR delle righe conserva le soluzioni, perché ripetendolo recuperiamo la vecchia riga. Questo procedimento permette anche di riconoscere una misura che ripete informazione già disponibile.

R_1, R_2 indicano le due righe della matrice. Tutte le somme sono XOR e il membro destro di ogni equazione è 0. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Una misura diversa può ripetere informazione già nota

Dopo le misure 010 e 111 abbiamo già ricostruito $s = 101$. Immaginiamo di proseguire e leggere 101 in A. Questa stringa compare per la prima volta nella sequenza, eppure la sua condizione si ottiene facendo XOR delle due condizioni già conservate.



$$\underbrace{010}_{\text{prima riga}} \oplus \underbrace{111}_{\text{seconda riga}} = \underbrace{101}_{\text{eventuale nuova misura}} .$$

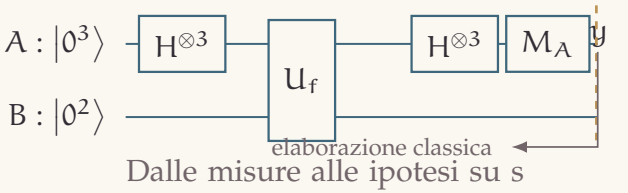
$$\underbrace{s_1}_{=0} \oplus \underbrace{(s_2 \oplus s_1 \oplus s_0)}_{=0} = s_2 \oplus s_0 = 0.$$

La riga 101 è lo XOR di 010 e 111 e aggiunge zero condizioni indipendenti. Il rango conta le condizioni indipendenti accumulate. Rileggiamo l'esecuzione completa distinguendo il numero di prove dal numero di righe utili.

Anche la riga 000 e una riga già letta sono dipendenti. Per decidere se una misura aggiunge informazione, controlliamo le sue combinazioni con le righe conservate. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Rango: numero di condizioni indipendenti.

Quattro esecuzioni, due condizioni, una stringa nascosta

Rileggiamo l'intero esempio: ogni risultato di A restringe l'elenco solo quando impone una condizione nuova. La stringa nascosta si ricostruisce combinando i risultati utili.



Esecuzione	Risultato misurato in A	Stringhe nascoste ancora possibili
1	000	001, 010, 011, 100, 101, 110, 111
2	010	001, 100, 101
3	010	001, 100, 101
4	111	**101**

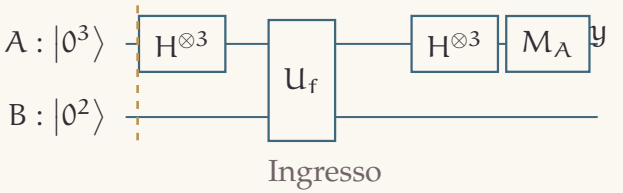
Verifica sulla tabella: $f(000) = f(101) = 00$, $000 \oplus 101 = 101$.

Quattro chiamate all'oracolo hanno prodotto due condizioni indipendenti e la risposta $s = 101$. Un risultato può quindi ripetere informazioni note. Nel prossimo esempio verificheremo anche che la stringa cercata può essere ricostruita pur avendo probabilità zero di comparire in misura.

Le quattro esecuzioni sono una possibile sequenza casuale. Le misure utili sono 010 e 111; la risposta cercata è la relazione XOR fra ingressi della stessa coppia. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

Possiamo ricostruire una stringa che non viene misurata?

Nel primo esempio a tre bit abbiamo distinto la stringa cercata dai risultati di A. Verifichiamo ora un caso più netto: la stringa nascosta sarà ricostruibile anche se non comparirà mai nella misura.



$$f(x_2x_1x_0) = (x_2 \oplus x_1,\ x_1 \oplus x_0).$$

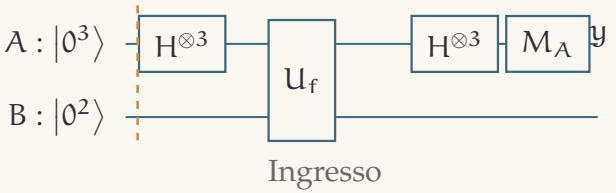
La prima componente dell'uscita è lo XOR del primo bit con il centrale; la seconda è lo XOR del centrale con l'ultimo. A contiene tre qubit, B due.

La nuova istanza ha stringa nascosta 111. Seguendo gli stessi passaggi, calcoleremo prima quali risultati può dare A e poi come usarli per ricostruire la risposta. Scriviamo la tabella della funzione e le sue coppie.

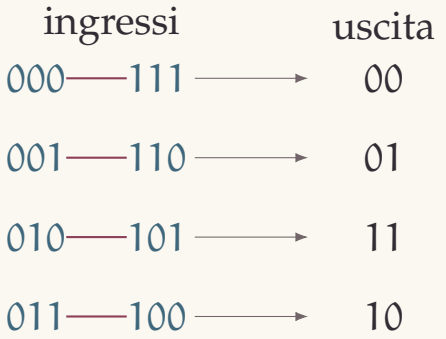
x_2 è il primo bit dell'ingresso, x_1 il centrale e x_0 l'ultimo. La tabella è disponibile al lettore per controllare i calcoli. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

La tabella della nuova funzione

Calcoliamo le due parità che compongono l'uscita. Le etichette raccolgono coppie di ingressi complementari, che differiscono in tutte e tre le posizioni.



x	f(x)
000	$(0 \oplus 0, 0 \oplus 0) = 00$
001	$(0 \oplus 0, 0 \oplus 1) = 01$
010	$(0 \oplus 1, 1 \oplus 0) = 11$
011	$(0 \oplus 1, 1 \oplus 1) = 10$
100	$(1 \oplus 0, 0 \oplus 0) = 10$
101	$(1 \oplus 0, 0 \oplus 1) = 11$
110	$(1 \oplus 1, 1 \oplus 0) = 01$
111	$(1 \oplus 1, 1 \oplus 1) = 00$

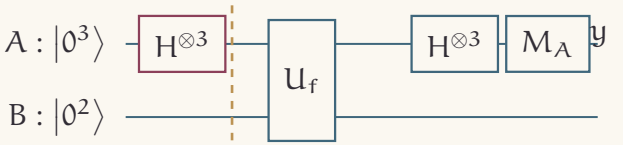


Le uscite individuano le quattro coppie indicate. Verifichiamo il loro XOR, poi prepariamo i tre qubit di A e i due di B.

La scatola nera calcola $f(x_2x_1x_0) = (x_2 \oplus x_1, x_1 \oplus x_0)$. Le due componenti dell'uscita occupano i due qubit di B. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

La promessa e la preparazione per 111

Le quattro coppie della tabella hanno tutte XOR uguale a 111. Dopo questo controllo prepariamo A, formato da tre qubit di ingresso, e B, formato da due qubit di uscita. La preparazione uniforme dipende dalle dimensioni dei registri e resta la stessa dell'esempio precedente:



Dopo le prime Hadamard

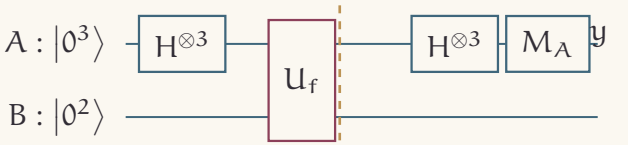
$$000 \oplus 111 = 111, \quad 001 \oplus 110 = 111,$$
$$010 \oplus 101 = 111, \quad 011 \oplus 100 = 111,$$
$$|\Psi_{\text{inizio}}\rangle = |000\rangle\,|00\rangle\,,$$
$$|\Psi_{\text{prep}}\rangle = \tfrac{1}{\sqrt{8}}(|000\rangle + |001\rangle + |010\rangle + |011\rangle$$
$$+ |100\rangle + |101\rangle + |110\rangle + |111\rangle)\,|00\rangle\,.$$

Tutte le coppie hanno XOR 111. La preparazione uniforme produce ancora otto ingressi con ampiezza $1/\sqrt{8}$. L'oracolo scriverà in B i valori della nuova tabella, così potremo selezionare una coppia e trasformarla.

Il lettore verifica $s = 111$ dalle coppie. Il circuito parte da $|000\rangle_A\,|00\rangle_B$ e assegna a ogni ingresso di A ampiezza $1/\sqrt{8}$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Lo stato congiunto per la stringa 111

La scatola nera scrive in B le due parità della nuova funzione.
Raccogliamo subito i termini con la stessa uscita: ciascuna etichetta di B corrisponde a due ingressi di A.



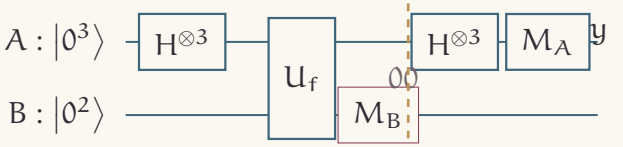
$$
\begin{aligned}
U_f\,|x, 00\rangle &= |x, f(x)\rangle\,, \\
|\Psi\rangle &= \tfrac{1}{\sqrt{8}}(|000, 00\rangle + |001, 01\rangle + |010, 11\rangle + |011, 10\rangle \\
&\qquad + |100, 10\rangle + |101, 11\rangle + |110, 01\rangle + |111, 00\rangle) \\
&= \tfrac{1}{\sqrt{8}}\big[(|000\rangle + |111\rangle)\,|00\rangle + (|001\rangle + |110\rangle)\,|01\rangle \\
&\qquad + (|010\rangle + |101\rangle)\,|11\rangle + (|011\rangle + |100\rangle)\,|10\rangle\big].
\end{aligned}
$$

La lettura $B = 00$ seleziona gli ingressi 000 e 111. Seguiamo questo ramo per calcolare gli esiti di A.
Confronteremo poi tutte le coppie per stabilire la distribuzione complessiva.

In $|x, c\rangle$, x è l'ingresso di tre bit conservato in A; $c = f(x)$ è l'uscita di due bit registrata in B. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=00 seleziona 000 e 111

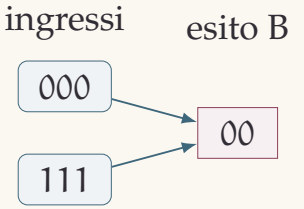
In questa istanza A contiene tre qubit di ingresso e B due qubit di uscita. Supponiamo di leggere 00 in B. I termini compatibili hanno ingressi 000 e 111, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità e normalizziamo A:



Lettura di B: coppia selezionata

$$P(B=00) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B=00)} = \frac{1}{2},$$

$$|\phi_{B=00}\rangle = \frac{(|000\rangle + |111\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|000\rangle + |111\rangle)$$
$$= \frac{|000\rangle + |111\rangle}{\sqrt{2}}.$$



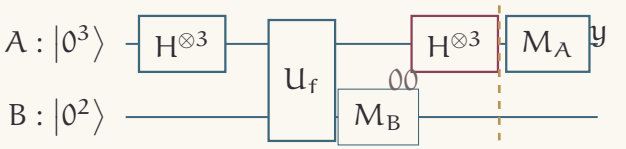
L'esito di B seleziona la coppia di ingressi.

A è nello stato $(|000\rangle + |111\rangle)/\sqrt{2}$. Sviluppiamo le due trasformate complete e sommiamole, come nel primo esempio.

Dopo aver letto B = 00, lo stato di A è $(|000\rangle + |111\rangle)/\sqrt{2}$. Ogni contributo finale ha fattore $(1/\sqrt{2})(1/\sqrt{8}) = 1/4$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 000 e 111

Dopo la lettura B = 00, A è nello stato $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|000\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle\Big],$$

$$H^{\otimes 3}|111\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle\Big].$$

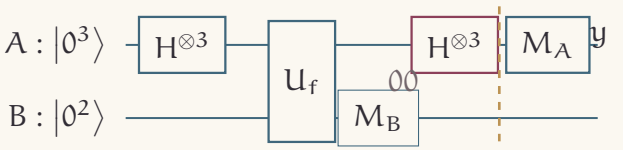
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 000 e 111

Sommiamo le due espansioni di $\frac{|000\rangle+|111\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|000\rangle + |111\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\left[\begin{array}{llll} (1+1)|000\rangle & + (1-1)|001\rangle & + (1-1)|010\rangle & + (1+1)|011\rangle \\ + (1-1)|100\rangle & + (1+1)|101\rangle & + (1+1)|110\rangle & + (1-1)|111\rangle \end{array}\right]$$

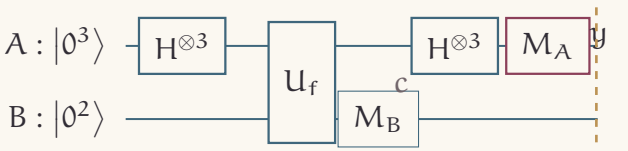
$$= \frac{2|000\rangle + 2|011\rangle + 2|101\rangle + 2|110\rangle}{4} = \frac{|000\rangle + |011\rangle + |101\rangle + |110\rangle}{2}.$$

Le quattro ampiezze valgono $1/2$, quindi ciascun risultato ha probabilità $(1/2)^2 = 1/4$. Anche il ket $|111\rangle$ si è cancellato.

A è il registro che misureremo. Qui B ha dato 00. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le quattro coppie dell'esempio 111

Ciascuna uscita di B ha probabilità 1/4 e seleziona una coppia. La tabella riporta le ampiezze di A dopo le Hadamard. Le quattro componenti non elencate sono zero.



Misura di A: risultato y

Uscita di B	Ingressi selezionati	A = 000 ampiezza	A = 011 ampiezza	A = 101 ampiezza	A = 110 ampiezza
00	000, 111	+1/2	+1/2	+1/2	+1/2
01	001, 110	+1/2	−1/2	−1/2	+1/2
11	010, 101	+1/2	−1/2	+1/2	−1/2
10	011, 100	+1/2	+1/2	−1/2	−1/2

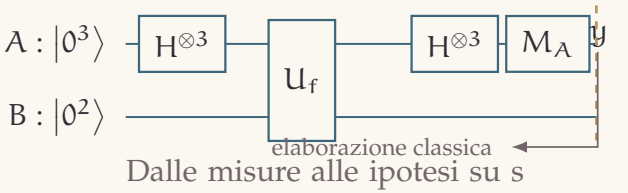
$$P(A = y) = 4 \cdot \underbrace{\tfrac{1}{4}}_{\text{probabilità di B}} \cdot \underbrace{(\tfrac{1}{2})^2}_{\text{probabilità di A dato B}} = \tfrac{1}{4}.$$

Ogni coppia dà quattro risultati con probabilità 1/4, mentre 111 ha probabilità zero. Supponiamo di leggere 011 e confrontiamo le sette ipotesi su s.

Conti completi: slide 169–177. Ogni riga descrive una coppia selezionata. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$.

La misura 011 lascia tre possibili stringhe nascoste

Supponiamo di misurare A = 011. Calcoliamo l'ampiezza in ciascuna coppia normalizzata, sommando due contributi di modulo 1/4. Contano il bit centrale e l'ultimo: cambiare una sola di queste posizioni inverte il segno, cambiarle entrambe o nessuna lo conserva.



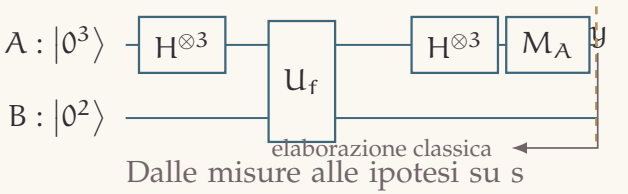
Stringhe nascoste ipotizzate	Cambi nelle ultime due posizioni	Ampiezza nella coppia normalizzata per A = 011	Compatibili con la misura?
001, 010, 101, 110	Uno	$\frac{1}{4} - \frac{1}{4} = 0$	No
100	Nessuno	$\pm(\frac{1}{4} + \frac{1}{4}) = \pm\frac{1}{2}$	Sì
011, 111	Due	$\pm(\frac{1}{4} + \frac{1}{4}) = \pm\frac{1}{2}$	Sì

Le ipotesi 001, 010, 101, 110 cancellerebbero 011 in ogni coppia e vengono escluse. Restano 011, 100, 111, nelle quali gli ultimi due bit sono uguali. Prepariamo di nuovo i registri e cerchiamo un risultato che distingua queste tre possibilità.

I due ingressi di una coppia hanno la stessa uscita della funzione. Nello stato normalizzato ciascuno pesa $1/\sqrt{2}$: dopo le tre Hadamard, ogni contributo vale $\pm(1/\sqrt{2})(1/\sqrt{8}) = \pm 1/4$. La promessa esclude la stringa nascosta 000. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

La misura 101 distingue i tre candidati rimasti

Una successiva esecuzione restituisce A = 101. Riprendiamo le tre ipotesi rimaste e sommiamo i contributi nella coppia normalizzata. Per questo risultato contano il primo e l'ultimo bit dell'ingresso.



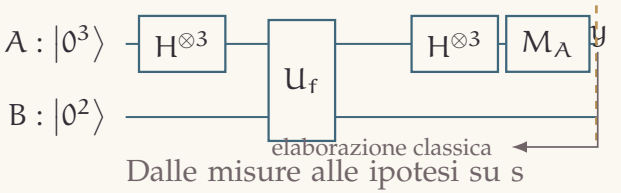
Stringa nascosta ipotizzata	Cambi nella prima e nell'ultima posizione	Ampiezza nella coppia normalizzata per A = 101	Compatibile con la misura?
011	Solo l'ultima	$\frac{1}{4} - \frac{1}{4} = 0$	No
100	Solo la prima	$\frac{1}{4} - \frac{1}{4} = 0$	No
111	Entrambe	$\pm(\frac{1}{4} + \frac{1}{4}) = \pm\frac{1}{2}$	Sì

Le ipotesi 011 e 100 cancellerebbero il risultato osservato 101. Rimane soltanto $s = 111$, compatibile con entrambe le misure. Riscriviamo sui singoli bit le due condizioni che hanno consentito questa ricostruzione.

I due ingressi di una coppia hanno la stessa uscita della funzione. Nello stato normalizzato ciascuno pesa $1/\sqrt{2}$: dopo le tre Hadamard, ogni contributo vale $\pm(1/\sqrt{2})(1/\sqrt{8}) = \pm 1/4$. La stringa ricostruita è 111, mentre le misure utili sono 011 e 101. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

Le due misure impongono che i tre bit siano uguali

Scriviamo le condizioni appena verificate. Le posizioni della stringa nascosta sono s_2 (prima), s_1 (centrale), s_0 (ultima). La misura 011 lega le ultime due; la misura 101 lega la prima e l'ultima.



$$A = 011: \quad s_1 \oplus s_0 = 0 \implies s_1 = s_0,$$
$$A = 101: \quad s_2 \oplus s_0 = 0 \implies s_2 = s_0.$$

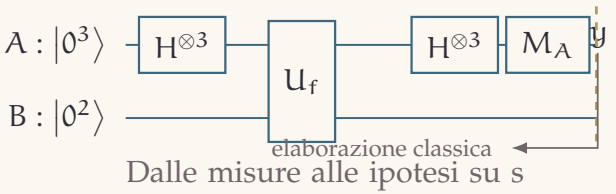
$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \begin{pmatrix} s_2 \\ s_1 \\ s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \implies s \in \{000, 111\} \implies \boxed{s = 111}.$$

La prima condizione rende uguali gli ultimi due bit, la seconda rende uguali il primo e l'ultimo. Restano 000 e 111. La promessa esclude 000, quindi ritroviamo $s = 111$. Il confronto fra le ipotesi e il sistema di equazioni descrivono la stessa inferenza.

Le righe della matrice sono i risultati misurati 011 e 101; le colonne seguono l'ordine primo, centrale, ultimo bit nascosto. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

Abbiamo ricostruito 111 senza averlo misurato

Riuniamo i risultati dell'esempio. Le misure possibili di A sono 000, 011, 101 e 110; ciascuna ha probabilità 1/4. La stringa nascosta 111 non compare in questo elenco.



Risultato misurato in A	Stringhe nascoste ancora possibili
011	011, 100, 111
101	111

Nella coppia 000, 111 : ampiezza di $|111\rangle = \dfrac{1-1}{4} = \dfrac{0}{4} = 0.$

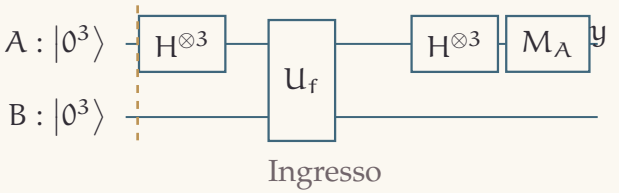
Verifica della risposta: $f(000) = f(111) = 00, \qquad 000 \oplus 111 = 111.$

Le due condizioni hanno ricostruito la stringa nascosta 111, che ha probabilità zero nella misura. Prima del caso generale, verifichiamo che cosa cambia assegnando nuove etichette alle coppie in B.

Il confronto fra tutte le uscite di B ha già mostrato che la cancellazione di A = 111 vale per ogni coppia. I conti completi sono in appendice. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Cambiare le etichette conserva le coppie di ingressi

Torniamo alla funzione con stringa nascosta 101. Definiamo una nuova scatola nera che assegna una nuova etichetta a ciascuna delle stesse quattro coppie. Le nuove etichette usano tre bit, quindi ora B contiene tre qubit.



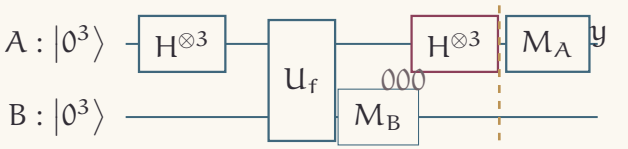
Ingressi della coppia	Vecchia uscita di B	Nuova uscita di B
000, 101	00	000
001, 100	01	001
010, 111	10	010
011, 110	11	100

Le nuove etichette restano distinte, quindi conservano esattamente le stesse coppie di ingressi. Il loro XOR è ancora 101. Confrontiamo gli stati di A selezionati dalla vecchia e dalla nuova etichetta della prima coppia.

La nuova funzione è $f' = g \circ f$, con $g(00) = 000$, $g(01) = 001$, $g(10) = 010$, $g(11) = 100$. Il nuovo formato di B è un dato dell'esempio. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Le Hadamard dipendono dagli ingressi della coppia

La vecchia uscita B = 00 e la nuova uscita B = 000 selezionano entrambe $(|000\rangle + |101\rangle)/\sqrt{2}$. Le due trasformate sono quelle già svolte alla slide 102. Sommiamole di nuovo: cambiare l'etichetta di B conserva tutti questi contributi.



Dopo le Hadamard finali

$$\mathrm{H}^{\otimes 3}\frac{|000\rangle + |101\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\left[\begin{array}{llll} (1+1)\,|000\rangle & + (1-1)\,|001\rangle & + (1+1)\,|010\rangle & + (1-1)\,|011\rangle \\ + (1-1)\,|100\rangle & + (1+1)\,|101\rangle & + (1-1)\,|110\rangle & + (1+1)\,|111\rangle \end{array}\right]$$

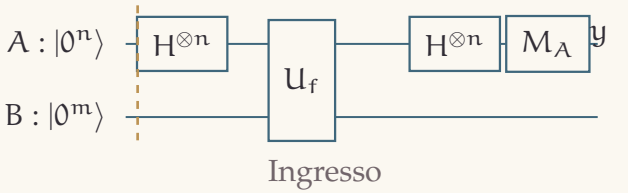
$$= \frac{2\,|000\rangle + 2\,|010\rangle + 2\,|101\rangle + 2\,|111\rangle}{4} = \frac{|000\rangle + |010\rangle + |101\rangle + |111\rangle}{2}.$$

Rimangono gli stessi quattro ket, con ampiezza 1/2 e probabilità 1/4 ciascuno. I conti delle altre coppie sono alle slide 161–168. Seguiamo ora il caso generale in sei passaggi, dall'ingresso alla ricostruzione di s.

Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma +2 oppure −2. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

1. L'ingresso: che cosa vogliamo ricostruire

Gli esempi hanno ricostruito la stringa nascosta combinando le misure di A. Seguiamo ora lo stesso circuito con n bit di ingresso. La funzione assegna la stessa uscita esattamente a due ingressi, collegati da una stringa fissa $s \neq 0^n$ che dobbiamo trovare.



$$f(x) = f(z) \quad \Longleftrightarrow \quad z = x \text{ oppure } z = x \oplus s.$$

Prepariamo A con n qubit tutti a zero. Prepariamo B con m qubit tutti a zero, pronti a ricevere il valore della funzione:

$$|\Psi_0\rangle = |0^n\rangle_A |0^m\rangle_B , \qquad U_f |x\rangle_A |t\rangle_B = |x\rangle_A |t \oplus f(x)\rangle_B .$$

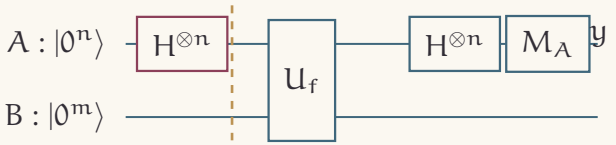
L'oracolo conserva l'ingresso x e aggiunge il valore f(x) al contenuto t di B. Con $t = 0^m$, il registro B riceverà proprio f(x).

Per interrogare la funzione su una sovrapposizione di ingressi, applichiamo prima una Hadamard a ciascun qubit di A. B resta nello stato iniziale.

A: registro degli ingressi, n qubit. B: registro dei valori di f, m qubit. $s \neq 0^n$: stringa nascosta. 0^n: stringa di n zeri. XOR ($\oplus$): somma bit per bit modulo 2, con $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile f. Promessa: proprietà della funzione garantita dal problema. Le coppie sono $2^n/2 = 2^{n-1}$ e richiedono altrettante etichette distinte in B. Nel circuito, M_A indica la misura di A. La linea oro indica il punto raggiunto.

2. Le prime Hadamard preparano tutti gli ingressi

Partiamo da $|\Psi_0\rangle = |0^n\rangle_A |0^m\rangle_B$. Ogni Hadamard trasforma uno zero in $(|0\rangle + |1\rangle)/\sqrt{2}$. Moltiplichiamo i n fattori: ogni scelta di uno zero o di un uno in ciascuna posizione produce una stringa x.



Dopo le prime Hadamard

$$
\begin{aligned}
|\Psi_1\rangle &= \left(H|0\rangle\right)^{\otimes n} |0^m\rangle_B = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes n} |0^m\rangle_B \\
&= \frac{1}{(\sqrt{2})^n}\left(|00\cdots0\rangle + |00\cdots1\rangle + \cdots + |11\cdots1\rangle\right)_A |0^m\rangle_B \\
&= \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle_A |0^m\rangle_B \,.
\end{aligned}
$$

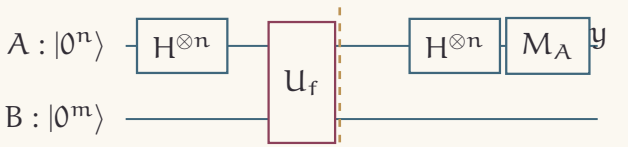
Ogni ingresso ha ampiezza $1/\sqrt{2^n}$. Le probabilità sommano a $2^n|1/\sqrt{2^n}|^2 = 2^n/2^n = 1$.

Applichiamo una volta l'oracolo: accanto a ciascun ingresso x comparirà il valore f(x).

A: registro degli ingressi, n qubit. B: registro dei valori di f, m qubit. $s \neq 0^n$: stringa nascosta. 0^n: stringa di n zeri. XOR ($\oplus$): somma bit per bit modulo 2, con $1 \oplus 1 = 0$. $\sum_x$ percorre tutte le stringhe di n bit. $H^{\otimes n}$ applica H a ciascun qubit. Il prodotto tensoriale combina i registri e moltiplica le ampiezze. Ampiezza: coefficiente dello stato.

3. L'oracolo associa ogni ingresso alla sua uscita

La preparazione ha dato $|\Psi_1\rangle = 2^{-n/2} \sum_x |x\rangle_A |0^m\rangle_B$. Trasformiamo ogni termine con $U_f |x\rangle |0^m\rangle = |x\rangle |f(x)\rangle$. Poi raccogliamo gli ingressi che hanno la stessa uscita, come negli esempi.



Dopo l'oracolo

$$|\Psi_2\rangle = U_f |\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_x |x\rangle_A |f(x)\rangle_B .$$

Chiamiamo c un valore distinto della funzione e u_c uno dei suoi due ingressi. L'altro è $u_c \oplus s$, perché $f(u_c) = f(u_c \oplus s) = c$. Quindi

$$|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_c \left(|u_c\rangle + |u_c \oplus s\rangle\right)_A |c\rangle_B .$$

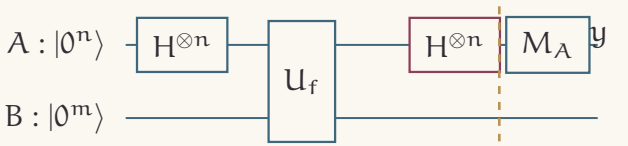
Ogni parentesi raccoglie due dei 2^n ingressi. Le etichette c sono dunque $2^n/2 = 2^{n-1}$. Il raggruppamento riscrive lo stesso stato congiunto.

B resta senza misura. Applichiamo le Hadamard ad A: per ciascuna etichetta c, i due ingressi della coppia contribuiranno allo stesso risultato finale y.

A: registro degli ingressi, n qubit. B: registro dei valori di f, m qubit. $s \neq 0^n$: stringa nascosta. 0^n: stringa di n zeri. XOR ($\oplus$): somma bit per bit modulo 2, con $1 \oplus 1 = 0$. c indica un valore distinto di f. u_c indica uno dei due ingressi che danno c. La somma su c contiene una sola volta ogni coppia. Linearità: si trasforma ogni termine e si sommano le immagini con gli stessi coefficienti.

4. Le Hadamard sommano i contributi di ogni coppia

Nello stato dopo l'oracolo, ogni etichetta c accompagna $|u_c\rangle + |u_c \oplus s\rangle$. Per un ingresso x, le Hadamard danno $H^{\otimes n}|x\rangle = 2^{-n/2}\sum_y (-1)^{x\cdot y}|y\rangle$. Applichiamo questa formula ai due termini della coppia.



Dopo le Hadamard finali

$$|\Psi_3\rangle = \frac{1}{2^n}\sum_c \sum_y \left[(-1)^{u_c\cdot y} + (-1)^{(u_c\oplus s)\cdot y}\right]|y\rangle_A\,|c\rangle_B\,.$$

Il fattore è $(1/\sqrt{2^n})(1/\sqrt{2^n}) = 1/2^n$. Poiché $(u_c \oplus s)\cdot y = (u_c\cdot y)\oplus(s\cdot y)$, raccogliamo il primo segno. Il coefficiente di $|y\rangle_A|c\rangle_B$ è

$$\alpha_{y,c} = \frac{(-1)^{u_c\cdot y}}{2^n}\left[1 + (-1)^{s\cdot y}\right].$$

La parentesi contiene proprio la somma dei due contributi:

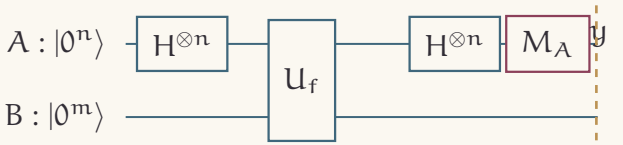
$$s\cdot y = 1: \quad \boxed{1-1} = 0, \qquad s\cdot y = 0: \quad \boxed{1+1} = 2.$$

Per $s\cdot y = 1$ i due contributi si cancellano per ogni c. Per $s\cdot y = 0$ rimane un'ampiezza $\alpha_{y,c} = \pm 2/2^n$. Calcoliamo la probabilità di leggere y nel registro A.

y: possibile risultato di A. c: valore nel registro B. $x\cdot y = x_{n-1}y_{n-1}\oplus\cdots\oplus x_0y_0$, somma dei prodotti modulo 2. La distributività dello XOR dà l'identità usata. $(-1)^0 = 1$, $(-1)^1 = -1$. Rosso: cancellazione. Blu: somma costruttiva, anche con segno comune negativo.

5. Ogni misura fornisce una condizione su s

Dopo le Hadamard il coefficiente di $|y\rangle_A |c\rangle_B$ è zero se $s \cdot y = 1$, oppure $\pm 2/2^n$ se $s \cdot y = 0$. Misuriamo soltanto A. Il risultato y può accompagnarsi a ciascuna delle 2^{n-1} etichette distinte di B.



Misura di A: risultato y

Per ottenere la probabilità di y sommiamo le probabilità dei termini con le diverse etichette c:

$$P(A = y) = \sum_c |\alpha_{y,c}|^2$$

$$= \begin{cases} 0, & s \cdot y = 1, \\ 2^{n-1} \left(\frac{2}{2^n}\right)^2 = \frac{2^{n-1}\,4}{2^{2n}} = \frac{1}{2^{n-1}}, & s \cdot y = 0. \end{cases}$$

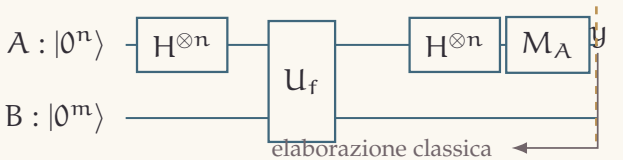
La stringa nascosta ha almeno un bit uguale a uno. Nell'equazione $y \cdot s = 0$, quel bit di y è determinato dagli altri $n - 1$: ci sono 2^{n-1} risultati ammessi, tutti con la stessa probabilità.

La stringa y letta in A impone quindi $y_{n-1}s_{n-1} \oplus \cdots \oplus y_0 s_0 = 0$. Ripetiamo il circuito per raccogliere altre equazioni e ricostruire la stringa nascosta s.

y: stringa misurata. s: stringa nascosta. Le diverse etichette c identificano stati distinti e ortogonali di B, quindi si sommano i moduli quadri dei coefficienti. Regola di Born: probabilità uguale al modulo quadro dell'ampiezza. Parità: somma dei bit modulo 2, uguale a 0 se il numero di bit 1 è pari.

6. Il sistema lineare ricostruisce la stringa nascosta

L'esecuzione i restituisce la stringa misurata $y^{(i)}$, che impone $y^{(i)} \cdot s = 0$. Raccogliamo r misure nelle righe della matrice Y. Le incognite sono i bit della stringa nascosta $s = s_{n-1} \cdots s_0$.



Sistema lineare: ricostruzione di s

$$\begin{cases} y^{(1)}_{n-1} s_{n-1} \oplus \cdots \oplus y^{(1)}_0 s_0 = 0, \\ \vdots \\ y^{(r)}_{n-1} s_{n-1} \oplus \cdots \oplus y^{(r)}_0 s_0 = 0 \end{cases} \iff \quad Y s = 0.$$

Combiniamo le righe con lo XOR, come per $010 \oplus 111 = 101$. Una riga nulla o ricavabile dalle precedenti aggiunge zero condizioni: la scartiamo e ripetiamo il circuito. Ogni condizione indipendente determina un bit in funzione degli altri. Quindi con k condizioni indipendenti restano $n - k$ bit liberi, ciascuno con due scelte, e quindi 2^{n-k} soluzioni.

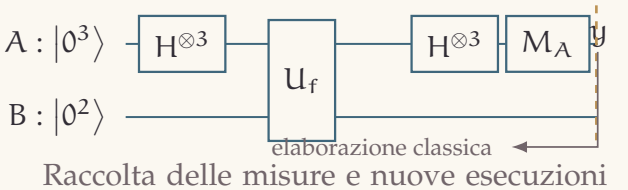
Con $k = n - 1$ resta un bit libero: le due soluzioni sono 0^n e s. La promessa esclude 0^n, quindi la soluzione non nulla è la stringa cercata.

Contiamo ora le prove necessarie per ottenere le n meno una condizioni indipendenti.

Tutte le somme nel sistema sono XOR. Condizione indipendente: non si ottiene facendo XOR delle altre condizioni raccolte. Rango k: numero di righe indipendenti. Bit libero: incognita che può valere 0 o 1 e determina poi le altre. Per n=1 la promessa lascia già la sola stringa s=1 e bastano zero misure.

Quali misure aggiungono informazione nell'esempio 101

Abbiamo stabilito quando fermarci. Per contare le prove, torniamo all'esempio $s = 101$: A dà $000, 010, 101, 111$, ciascuno con probabilità $1/4$. All'inizio serve un risultato non nullo. Dopo 010, le letture 000 e 010 ripetono informazione già disponibile.



Righe raccolte	Risultati che ripetono	Risultati utili
Nessuna	000	010, 101, 111
010	000, 010	101, 111
010, 111	000, 010, 101, 111	Nessuno: ricerca conclusa

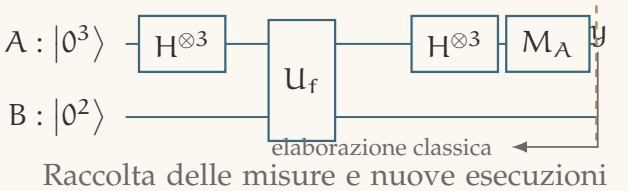
$$P(\text{prima condizione utile}) = \frac{3}{4}, \qquad P(\text{seconda} \mid \text{prima acquisita}) = \frac{2}{4} = \frac{1}{2}.$$

Dopo due righe indipendenti, anche $101 = 010 \oplus 111$ è già ricavabile. Per trovare il numero medio di prove sommiamo l'attesa della prima condizione e quella della seconda.

Una condizione utile è indipendente dalle precedenti. In aritmetica binaria i multipli di una riga sono soltanto la riga stessa e la riga nulla. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

L'attesa media per le due condizioni

Chiamiamo E_p il numero medio di prove necessarie per ottenere un successo quando ogni prova ha probabilità p. Eseguiamo una prova. Se riesce abbiamo finito, se fallisce resta da attendere in media ancora E_p prove.



$$E_p = \underbrace{1}_{\text{prova eseguita}} + \underbrace{p \cdot 0}_{\text{successo}} + \underbrace{(1-p)E_p}_{\text{fallimento}},$$

$$E_p - (1-p)E_p = 1 \quad \Longrightarrow \quad pE_p = 1 \quad \Longrightarrow \quad E_p = \frac{1}{p},$$

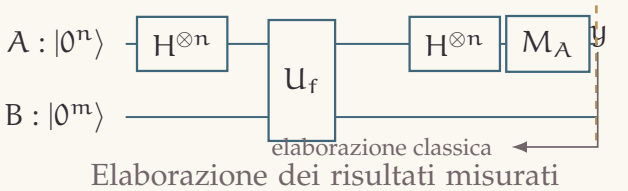
$$\mathbb{E}[T] = \frac{1}{3/4} + \frac{1}{1/2} = \frac{4}{3} + 2 = \frac{10}{3}.$$

Per tre bit servono quindi in media 10/3 prove. La probabilità di una nuova condizione cambia quando acquisiamo una riga utile. Per n bit dobbiamo contare gli esiti già ricavabili a ogni stadio.

$\mathbb{E}[T]$ è la media del numero totale T di prove. Le esecuzioni sono indipendenti: ogni volta i registri ripartono dalla stessa preparazione.

Con k righe conosciamo già due alla k combinazioni

Dopo aver raccolto k righe indipendenti, possiamo includere oppure escludere ciascuna riga da uno XOR. Le due scelte per ogni riga producono 2^k combinazioni distinte. I risultati possibili del circuito sono invece 2^{n-1} e hanno tutti la stessa probabilità.



Elaborazione dei risultati misurati

$$k = 2: \quad \{0, r_1, r_2, r_1 \oplus r_2\} \quad \text{contiene } 2 \cdot 2 = 4 \text{ righe,}$$

$$P(\text{condizione già nota}) = \frac{2^k}{2^{n-1}},$$

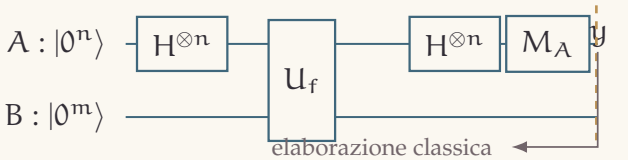
$$p_k = P(\text{nuova condizione}) = 1 - \frac{2^k}{2^{n-1}}.$$

Con n=3, per k=0 troviamo $1 - 1/4 = 3/4$ e per k=1 troviamo $1 - 2/4 = 1/2$. Ritroviamo le probabilità dell'esempio. Possiamo ora sommare le attese di tutte le fasi fino alle n meno una righe richieste.

Le combinazioni sono distinte perché le righe sono indipendenti. L'insieme di tutti i loro XOR si chiama spazio generato, o span. Il rango k conta le righe indipendenti. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Il numero medio di prove cresce al più linearmente

Prima dell'arresto abbiamo al massimo n meno due righe indipendenti. Di conseguenza almeno metà dei risultati possibili aggiunge una condizione. L'attesa media di ogni nuova riga è quindi al massimo due prove.



Elaborazione dei risultati misurati

$$k \leq n-2 \quad \Longrightarrow \quad \frac{2^k}{2^{n-1}} \leq \frac{1}{2},$$

$$p_k = 1 - \frac{2^k}{2^{n-1}} \geq \frac{1}{2} \quad \Longrightarrow \quad \frac{1}{p_k} \leq 2,$$

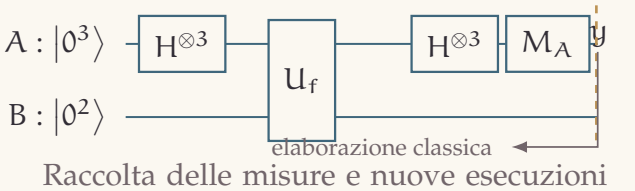
$$\mathbb{E}[T] = \sum_{k=0}^{n-2} \frac{1}{1-2^{k-(n-1)}} \leq \underbrace{2+2+\cdots+2}_{n-1 \text{ nuove righe}} = 2(n-1).$$

Questa è una media su molte esecuzioni complete. Se fissiamo in anticipo un numero di prove, possiamo invece calcolare la probabilità di aver già ricostruito s entro quel limite. Cominciamo da tre prove nell'esempio a tre bit.

"Lineare in n" significa proporzionale alla lunghezza della stringa, a meno di costanti. Ogni prova usa una chiamata all'oracolo. $\mathbb{E}[T]$ indica una media, non una garanzia. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

Tre prove possono lasciare una sola condizione

Nell'esempio $s = 101$, ogni prova dà uno dei quattro risultati $000, 010, 101, 111$. Per concludere servono due risultati non nulli diversi. La ricerca resta incompleta se tutte le misure sono nulle oppure se compare un solo tipo di risultato non nullo.



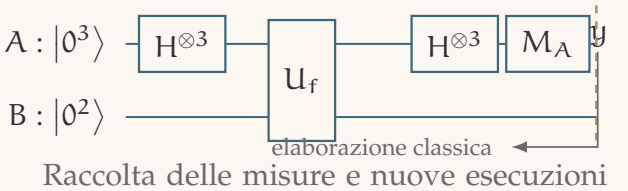
Unico risultato non nullo: 010	Sequenze incomplete con almeno un 010
Una comparsa	$(010, 000, 000)$, $(000, 010, 000)$, $(000, 000, 010)$
Due comparse	$(010, 010, 000)$, $(010, 000, 010)$, $(000, 010, 010)$
Tre comparse	$(010, 010, 010)$

Per il risultato non nullo 010 abbiamo contato sette sequenze. Anche 101 e 111 danno sette sequenze ciascuno. Questi tre gruppi sono distinti, perché in ognuno compare un unico tipo di risultato non nullo. Aggiungiamo poi la sequenza tutta nulla.

Le parentesi indicano i risultati della prima, seconda e terza prova. Due stringhe binarie non nulle diverse sono indipendenti: nessuna è zero o uguale all'altra.

Quarantadue sequenze su sessantaquattro bastano

Contiamo tutte le sequenze di tre prove e sottraiamo quelle incomplete appena elencate. Ogni prova ha quattro risultati equiprobabili e riparte dalla stessa preparazione.



$$\text{sequenze totali} = 4 \cdot 4 \cdot 4 = 64,$$

$$\text{sequenze incomplete} = \underbrace{1}_{\text{tutte nulle}} + \underbrace{3 \cdot 7}_{\text{un solo tipo non nullo}} = 22,$$

$$\text{sequenze sufficienti} = 64 - 22 = 42,$$

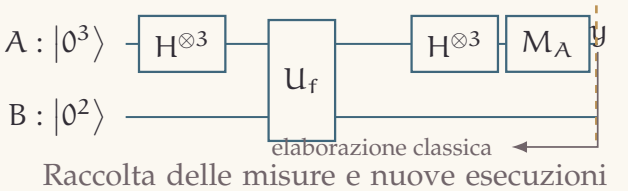
$$Q_3 = P(\text{ricostruzione entro 3 prove}) = 42 \left(\frac{1}{4}\right)^3 = \frac{42}{64} = \frac{21}{32}.$$

Abbiamo ottenuto la probabilità contando direttamente ciò che possiamo osservare. Per estendere il conteggio a n bit e r prove conviene rappresentare ogni risultato con i coefficienti necessari a comporlo. Introduciamo questa descrizione usando gli stessi quattro risultati.

Q_3 è la probabilità di avere già abbastanza condizioni entro tre prove. Le 64 sequenze hanno tutte probabilità 1/64. Il caso tutto nullo è contato una sola volta.

Due coefficienti descrivono i quattro risultati

Scegliamo le stringhe $v_1 = 010$ e $v_2 = 101$. Possiamo ottenere ogni risultato ammesso includendo oppure escludendo ciascuna di esse da uno XOR. I coefficienti a e b indicano queste due scelte.



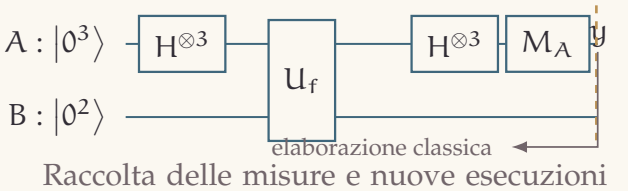
Risultato di A	$av_1 \oplus bv_2$	Coefficienti (a, b)
000	$0(010) \oplus 0(101)$	$(0, 0)$
010	$1(010) \oplus 0(101)$	$(1, 0)$
101	$0(010) \oplus 1(101)$	$(0, 1)$
111	$1(010) \oplus 1(101) = 010 \oplus 101$	$(1, 1)$

Le due stringhe scelte formano una base: sono indipendenti e permettono di ottenere ogni risultato ammesso. I due coefficienti sono le coordinate del risultato rispetto a questa base. La corrispondenza è uno a uno, quindi contare sequenze di coordinate equivale a contare sequenze di risultati.

Base: insieme indipendente che genera tutti i risultati considerati tramite XOR. Coordinate: coefficienti 0 o 1 delle stringhe della base. Il circuito continua a misurare tre bit. La base serve al conteggio nella dimostrazione e non deve essere nota all'algoritmo. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

La matrice delle coordinate serve a contare le sequenze

Per la sequenza di misure 010, 101, 111, le coordinate sono $(1,0),(0,1),(1,1)$. Le scriviamo in tre righe. Ogni colonna raccoglie l'uso di una delle due stringhe della base nelle tre prove.



$$C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{pmatrix}, \qquad c_1 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \qquad c_2 = \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}.$$

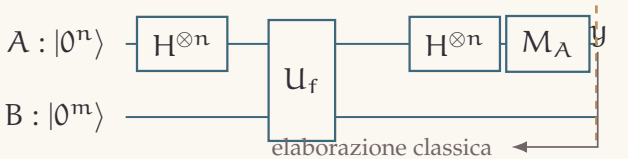
Caso insufficiente	Righe che possono comparire
$c_1 = 000$	$00, 01$
$c_2 = 000$	$00, 10$
$c_1 = c_2$	$00, 11$

In ciascun caso insufficiente compare al massimo una riga non nulla diversa. Per avere due condizioni indipendenti, le colonne devono essere non nulle e diverse. Fra gli otto valori possibili, la prima colonna ha sette scelte e la seconda sei: ritroviamo $7 \cdot 6 = 42$.

C contiene coordinate per contare le sequenze. Y contiene invece i bit realmente misurati per ricostruire s. Il rango conta le condizioni indipendenti in entrambe le descrizioni.

Il conteggio delle colonne per n bit e r prove

Con n bit servono $d = n - 1$ stringhe indipendenti per descrivere tutti i risultati ammessi. Una sequenza di r prove diventa quindi una matrice con r righe e d colonne. Per concludere servono d righe indipendenti, equivalenti a d colonne indipendenti.



Elaborazione dei risultati misurati

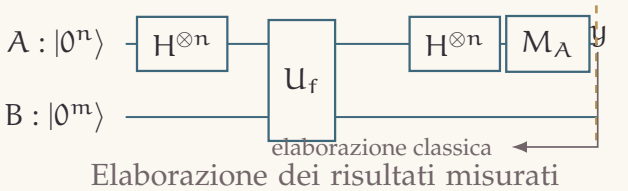
Colonna scelta	Valori da evitare	Scelte rimaste
Prima	La colonna nulla	$2^r - 1$
Seconda	$0, c_1$	$2^r - 2$
Terza	$0, c_1, c_2, c_1 \oplus c_2$	$2^r - 4$
Colonna $j + 1$	I 2^j XOR delle prime j colonne	$2^r - 2^j$

Ogni colonna ha r bit, quindi 2^r valori possibili. Scartiamo quelli già ottenibili dalle colonne precedenti. Moltiplicando le scelte rimaste contiamo le matrici che permettono di concludere. Dividiamo poi per il numero di tutte le matrici.

Il rango per righe e per colonne coincide: l'eliminazione individua lo stesso numero di pivot. Un pivot è un 1 che identifica una condizione indipendente. Qui assumiamo $r \geq d = n - 1$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

La probabilità di concludere entro r prove

Le d colonne hanno ciascuna 2^r valori possibili. Le matrici totali sono quindi $(2^r)^d$. Il conteggio precedente dà quelle con d condizioni indipendenti. Ogni matrice ha la stessa probabilità, perché ogni risultato ammesso è uniforme.



Elaborazione dei risultati misurati

$$Q_r = \frac{(2^r-1)(2^r-2)\cdots(2^r-2^{d-1})}{(2^r)^d}$$

$$= \left(1-\frac{1}{2^r}\right)\left(1-\frac{2}{2^r}\right)\cdots\left(1-\frac{2^{d-1}}{2^r}\right),$$

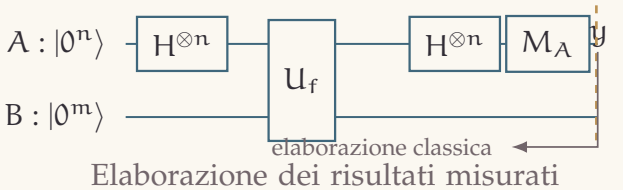
$$d=2,\ r=3: \quad Q_3 = \left(1-\frac{1}{8}\right)\left(1-\frac{2}{8}\right) = \frac{7}{8}\frac{6}{8} = \frac{42}{64}.$$

La formula generale restituisce il conteggio concreto dell'esempio. Per scegliere quante prove eseguire, cerchiamo ora un limite semplice alla probabilità di non aver ancora concluso, pari a $1 - Q_r$.

$d = n - 1$ è il numero di condizioni indipendenti richieste. Q_r è la probabilità di completamento entro r prove. Se $r < d$, le condizioni non possono bastare e $Q_r = 0$. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

La probabilità di insuccesso si limita con una somma

Il prodotto che dà Q_r può essere lungo. Per due fattori, sottrarlo da uno produce una somma meno un termine positivo. Il risultato è quindi al massimo la somma. Ripetiamo lo stesso ragionamento aggiungendo un fattore alla volta.



Elaborazione dei risultati misurati

$$1-(1-a)(1-b) = a+b-ab \le a+b, \qquad 0 \le a, b \le 1,$$

$$P_k = (1-a_0)\cdots(1-a_{k-1}), \qquad 0 \le P_k \le 1,$$

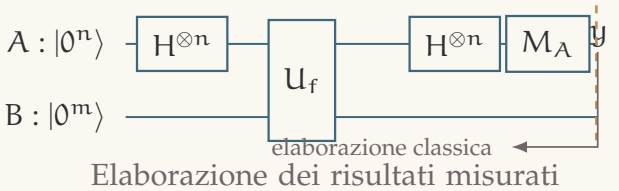
$$\begin{aligned} 1-P_k(1-a_k) &= (1-P_k) + P_k a_k \le (1-P_k) + a_k \\ &\le a_0 + \cdots + a_{k-1} + a_k. \end{aligned}$$

Con un solo fattore l'uguaglianza è esatta: $1-(1-a_0) = a_0$. Ogni fattore successivo aggiunge al limite al massimo il proprio a. Per Q_r questi valori sono $1/2^r, 2/2^r, \ldots, 2^{d-1}/2^r$. Sommiamoli.

Questa è una dimostrazione per induzione: si verifica il primo caso e si mostra che aggiungere un fattore conserva la proprietà. Per $r \ge d$, tutti gli a sono fra 0 e 1.

Le prove aggiuntive riducono il limite di insuccesso

La somma da calcolare è $(1 + 2 + \cdots + 2^{d-1})/2^r$. Chiamiamo S il numeratore. Sottraendolo dal suo doppio si cancellano tutti i termini intermedi, lasciando soltanto $2^d - 1$.



Elaborazione dei risultati misurati

$$S = 1 + 2 + \cdots + 2^{d-1},$$

$$2S = 2 + 4 + \cdots + 2^{d}, \qquad 2S - S = 2^d - 1,$$

$$1 - Q_r \le \frac{1 + 2 + \cdots + 2^{d-1}}{2^r} = \frac{2^d - 1}{2^r} < 2^{d-r},$$

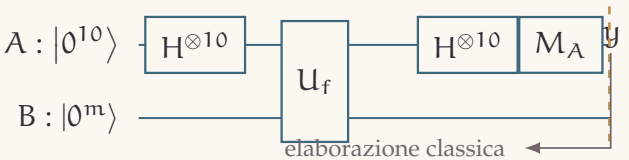
$$r = d + t: \quad 1 - Q_r < 2^{d-(d+t)} = 2^{-t}.$$

d è il numero di condizioni necessarie e t conta le prove eseguite oltre d. Ogni prova aggiuntiva dimezza questo limite superiore all'insuccesso. Usiamo alcuni valori numerici per scegliere un numero di esecuzioni.

Un limite superiore può essere più grande della probabilità effettiva. $1 - Q_r$ è la probabilità che le r prove raccolte non bastino ancora a ricostruire s.

Dieci bit: dalla soglia al numero di prove

Con n=10 servono $d = 9$ condizioni indipendenti. Scegliamo t prove aggiuntive e usiamo il limite $1 - Q_r < 2^{-t}$, con $r = 9 + t$.



Numero di esecuzioni per dieci bit

Prove aggiuntive t	Prove totali r	Limite all'insuccesso
3	$9 + 3 = 12$	$1/8 = 0.125$
7	$9 + 7 = 16$	$1/128 \simeq 0.0078$
21	$9 + 21 = 30$	$1/2097152 < 10^{-6}$

$$n \text{ qualsiasi}: \quad r = (n-1) + 21 = n + 20 \quad \Longrightarrow \quad 1 - Q_r < 10^{-6}.$$

Il limite permette di fissare il numero di prove prima dell'esecuzione. Alla fine controlliamo comunque quante condizioni indipendenti abbiamo raccolto. Passiamo ora a una ricerca classica casuale e contiamo le interrogazioni necessarie a trovare due ingressi con la stessa uscita.

Il rango conta le condizioni indipendenti. Se raggiunge $n - 1$, la ricostruzione è completa. La probabilità d'insuccesso riguarda il numero di prove fissato in anticipo.

Otto ingressi: la ricerca classica di una coppia

La strategia classica sceglie ingressi distinti a caso e confronta le uscite della scatola nera. Nell'esempio ci sono otto ingressi divisi in quattro coppie. Dopo j interrogazioni senza uscite uguali, restano da provare i j compagni degli ingressi già scelti.

Ingressi già provati j	Ingressi rimasti	Compagni fra i rimasti	Probabilità di trovarne uno
1	$8-1=7$	1	$1/7$
2	$8-2=6$	2	$2/6$
3	$8-3=5$	3	$3/5$
4	$8-4=4$	4	$4/4=1$

Il conteggio vale finché le uscite precedenti sono tutte diverse. I compagni esistono, ma la strategia non sa quali ingressi siano. Quando due uscite coincidono, lo XOR dei due ingressi restituisce s. Calcoliamo la probabilità di arrivare a quel momento entro tre, quattro e cinque interrogazioni.

Collisione: due ingressi distinti danno la stessa uscita. Per la promessa di Simon sono x e $x \oplus s$, quindi il loro XOR è s. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Tre, quattro e cinque interrogazioni classiche

Chiamiamo $P_0(q)$ la probabilità che q interrogazioni distinte non abbiano ancora prodotto una collisione. Il primo ingresso non può completare una coppia. Al secondo passo dobbiamo evitare un compagno su sette, al terzo due su sei.

$$P_0(3) = 1 \cdot \frac{6}{7} \cdot \frac{4}{6} = \frac{4}{7}, \qquad P(\text{collisione entro } 3) = 1 - \frac{4}{7} = \frac{3}{7},$$

$$P_0(4) = \frac{4}{7} \cdot \frac{2}{5} = \frac{8}{35}, \qquad P(\text{collisione entro } 4) = 1 - \frac{8}{35} = \frac{27}{35},$$

$$P_0(5) = \frac{8}{35} \cdot \frac{0}{4} = 0, \qquad P(\text{collisione entro } 5) = 1.$$

Cinque ingressi distinti devono completare almeno una delle quattro coppie. Dopo tre prove, la ricerca casuale aveva probabilità 3/7, mentre Simon aveva probabilità 21/32 di ricostruire s. Per capire come cresce il costo con n, estendiamo il conteggio a $N = 2^n$ ingressi.

Le frazioni sono probabilità condizionate all'assenza di collisioni precedenti. La loro moltiplicazione dà la probabilità che tutti i passi evitino una collisione. Collisione: due ingressi distinti producono la stessa uscita.

La probabilità classica con N ingressi

Dopo j interrogazioni senza collisioni restano $N - j$ ingressi. Esattamente j sono compagni di quelli già interrogati. Gli altri $N - 2j$ evitano una collisione. Moltiplichiamo questa probabilità per tutti i passi.

$$P(\text{evitare la collisione al passo } j+1) = \frac{N-2j}{N-j} = 1 - \frac{j}{N-j},$$

$$P_0(q) = \prod_{j=0}^{q-1} \left(1 - \frac{j}{N-j}\right),$$

$$P(\text{collisione entro } q) = 1 - P_0(q).$$

Il prodotto riassume lo stesso conto svolto con otto ingressi. Per stimare quanti accessi siano necessari, contiamo ora quante coppie di interrogazioni possono produrre una collisione.

$\prod$ indica la moltiplicazione di tutti i fattori. $N = 2^n$. La formula vale fino a $q = N/2 + 1$, quando la collisione è certa. La strategia sceglie ingressi distinti uniformemente a caso. Collisione: due ingressi distinti producono la stessa uscita.

Quante coppie possiamo confrontare

Fra q ingressi, ciascuno si confronta con altri q meno uno. Dividiamo per due perché ogni coppia è contata due volte. Fissato un ingresso, soltanto uno degli altri $N-1$ è il suo compagno.

$$\text{coppie di interrogazioni} = \frac{q(q-1)}{2},$$

$$P(\text{almeno una collisione}) \leq \frac{q(q-1)}{2(N-1)},$$

$$P(\text{collisione}) \geq \frac{1}{2} \implies q(q-1) \geq N-1$$

$$\implies q \geq \sqrt{N-1}.$$

Sommando le probabilità possiamo contare più volte una sequenza con più collisioni: otteniamo un limite superiore. Per successo almeno $1/2$ occorre quindi $q \geq \sqrt{N-1}$. Cerchiamo anche un numero sufficiente.

Limite dell'unione: la probabilità che si verifichi almeno uno fra più eventi è al massimo la somma delle loro probabilità. Qui gli eventi sono le possibili collisioni fra interrogazioni. Collisione: due ingressi distinti producono la stessa uscita.

Un limite alla probabilità di non trovare la coppia

Per avere un numero sufficiente di interrogazioni, cerchiamo un limite superiore a $P_0(q)$. Usiamo $1-u \le e^{-u}$ e sostituiamo ogni denominatore $N-j$ con N, ottenendo un limite più grande ma più semplice.

$$P_0(q) = \prod_{j=0}^{q-1}\left(1-\frac{j}{N-j}\right) \le \exp\left(-\sum_{j=0}^{q-1}\frac{j}{N-j}\right)$$
$$\le \exp\left(-\frac{1}{N}\sum_{j=0}^{q-1} j\right) = \exp\left(-\frac{q(q-1)}{2N}\right),$$

$$\exp\left(-\frac{q(q-1)}{2N}\right) \le \delta \quad\Longleftrightarrow\quad q(q-1) \ge 2N\ln(1/\delta).$$

Il simbolo δ indica la soglia di insuccesso desiderata. A soglia fissata, basta una quantità di interrogazioni proporzionale a $\sqrt{N}$. Traduciamo la formula in numeri per una stringa di dieci bit.

$\exp(z) = e^z$ e $\ln$ è il logaritmo naturale. Il grafico di e^{-u} sta sopra la tangente $1-u$, quindi $1-u \le e^{-u}$. Inoltre $\sum_{j=0}^{q-1} j = q(q-1)/2$.

Dieci bit: il confronto fra le interrogazioni

Confrontiamo i limiti sufficienti per n=10 e soglia di insuccesso $\delta = 1/8$. Simon richiede nove condizioni indipendenti e usa tre prove aggiuntive. Per la ricerca casuale abbiamo $N = 2^{10} = 1024$ ingressi.

$$\text{Simon:} \quad r = (10-1)+3 = 12, \qquad 1 - Q_{12} < 2^{-3} = \frac{1}{8},$$

$$\text{Ricerca casuale:} \quad 2N \ln(1/\delta) = 2048 \ln 8 \simeq 4258.70,$$

$$q = 66: \quad q(q-1) = 66 \cdot 65 = 4290 \geq 4258.70,$$

$$P_0(66) \leq 1/8.$$

I numeri indicano quantità sufficienti secondo i limiti dimostrati. Il confronto riguarda la ricerca classica casuale descritta e la sola promessa di Simon. Una conoscenza aggiuntiva della funzione può consentire una strategia classica diversa: vediamo un caso concreto.

δ è il massimo insuccesso ammesso. Una prova quantistica usa una chiamata all'oracolo. La scala classica casuale è $\sqrt{2^n} = 2^{n/2}$, mentre quella quantistica è lineare in n. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$. Condizione indipendente: non si ottiene facendo XOR delle precedenti.

Conoscere la forma della funzione cambia la strategia

Aggiungiamo l'ipotesi che la funzione sia lineare: $f(x) = Lx$, con somme binarie. Interrogando gli ingressi con un solo bit 1 leggiamo le colonne della matrice L. Nell'esempio $s = 101$ bastano questi tre ingressi.

$$f(100) = 01, \qquad f(010) = 10, \qquad f(001) = 01,$$

$$L = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}, \qquad Ls = \begin{pmatrix} s_1 \\ s_2 \oplus s_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

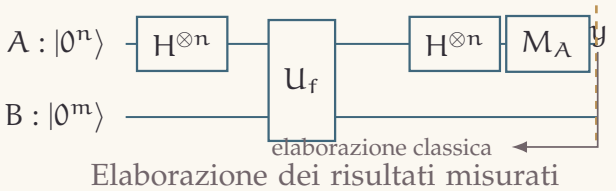
$$s_1 = 0, \quad s_2 = s_0 \quad \Longrightarrow \quad s \in \{000, 101\} \quad \Longrightarrow \quad s = 101.$$

La promessa esclude 000 e lascia 101. Questa ricostruzione usa l'informazione aggiuntiva che f è lineare. Gli oracoli concreti servono a verificare gli esempi, mentre il procedimento di Simon funziona usando la promessa sulle coppie. Completiamo ora il conto del lavoro classico successivo alle misure.

Funzione lineare binaria: $f(x \oplus z) = f(x) \oplus f(z)$. Le risposte a $100, 010, 001$ sono, nell'ordine, le tre colonne di L. La promessa impone $s \neq 000$. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$.

Quanto lavoro richiede controllare una nuova misura

Per decidere se una misura aggiunge informazione, cancelliamo i suoi bit usando i pivot delle righe già conservate. Nell'esempio ridotto le righe sono 101 e 010. Una nuova misura 111 si elimina con due XOR.



$$111 \oplus 101 = 010, \qquad 010 \oplus 010 = 000,$$

$$\text{un XOR fra due righe di n bit :} \quad n \text{ operazioni sui bit,}$$

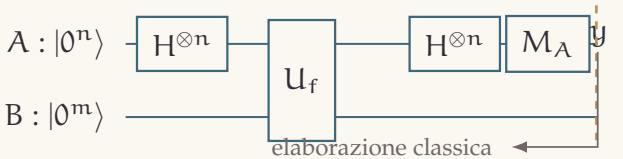
$$\text{al massimo n righe da usare :} \quad n \cdot n = n^2 \text{ operazioni.}$$

Il residuo nullo conferma che la condizione era già disponibile. Il costo per controllare una misura cresce al più come n^2. Moltiplichiamolo per il numero medio di prove e aggiungiamo la risoluzione finale delle equazioni.

Pivot: primo bit 1 di una riga ridotta, usato per cancellare la stessa posizione nelle altre righe. XOR fra righe equivale a sommare le equazioni modulo 2.

Le risorse del procedimento completo

Il controllo di ogni misura costa al più dell'ordine di n^2 operazioni. Moltiplichiamo per il numero medio di prove. La risoluzione finale usa al più n passi, ciascuno con n XOR su n bit.



Elaborazione dei risultati misurati

$$n^2\mathbb{E}[T] \le 2n^2(n-1) = O(n^3), \qquad n \cdot n \cdot n = O(n^3).$$

Risorsa	Quantità
Qubit	$n + m$
Chiamate all'oracolo per prova	1
Hadamard per prova	$2n$
Chiamate medie	$\le 2(n-1)$
Operazioni classiche medie sui bit	$O(n^3)$

Il costo di realizzare l'oracolo si aggiunge alle risorse elencate. Concludiamo confrontando il significato della risposta di Simon con quella di Bernstein–Vazirani.

$O(n^3)$ indica una crescita al massimo proporzionale a n^3 per n grande, trascurando costanti. n è il numero di bit di ingresso, m quello dei bit di uscita. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f.

La stessa stringa in due problemi distinti

Confrontiamo le due ricostruzioni già svolte per s=101. La stringa ha lunghezza uguale, mentre le funzioni la definiscono attraverso proprietà diverse. Anche la dimensione del registro d'uscita riflette questa differenza.

$$\text{BV:} \quad f_s(x) = x_2 \oplus x_0 \in \{0,1\}, \quad m = 1,$$

$$\text{Simon:} \quad f(x) = (x_1, x_2 \oplus x_0) \in \{0,1\}^2, \quad m = 2.$$

$$\text{BV: } U_f |x\rangle |-\rangle = (-1)^{f(x)} |x\rangle |-\rangle ,$$

$$\text{Simon: } U_f |x\rangle |0^m\rangle = |x\rangle |f(x)\rangle .$$

BV: coefficienti della parità

↓

Stringa cercata in entrambi: 101

↓

Simon: relazione XOR fra ingressi

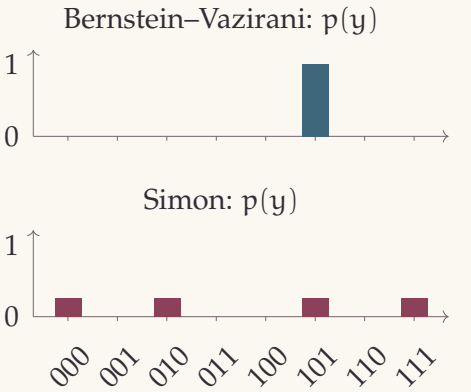
In Bernstein–Vazirani i bit di 101 selezionano il primo e l'ultimo termine della parità. In Simon, 101 collega ingressi con la stessa uscita. Confrontiamo le distribuzioni che i due circuiti hanno prodotto per queste due funzioni.

In entrambi gli esempi s = 101. BV usa $f_s(x) = x_2 \oplus x_0$; Simon usa $f(x) = (x_1, x_2 \oplus x_0)$. In BV, $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le distribuzioni dei risultati osservati

Ripresentiamo le distribuzioni complete calcolate nei due esempi. Questa lettura consente di verificare quale informazione sia disponibile dopo una singola esecuzione del circuito.

y	BV: $p(y)$	Simon: $p(y)$
000	0	1/4
001	0	0
010	0	1/4
011	0	0
100	0	0
101	1	1/4
110	0	0
111	0	1/4



Bernstein–Vazirani restituisce 101 con probabilità uno. Simon restituisce 000, 010, 101, 111, ciascuno con probabilità 1/4. Per leggere la risposta di Simon dobbiamo usare gli esiti come coefficienti delle condizioni su s. Riprendiamo le due misure utili dell'esempio.

Dati: BV $f_s(x) = x_2 \oplus x_0$; Simon $f(x) = (x_1, x_2 \oplus x_0)$; stringa dell'istanza 101.

La ricostruzione finale nei due procedimenti

Completiamo il confronto seguendo la risposta fino al suo significato iniziale. La procedura classica successiva alla misura dipende dall'informazione che il circuito rende accessibile.

$$\begin{aligned} \text{BV:}\quad & y = 101 \quad \Longrightarrow \quad s = 101, \\ \text{Simon:}\quad & y^{(1)} = 010,\ y^{(2)} = 111 \\ \Longrightarrow\quad & s_1 = 0,\ s_2 \oplus s_1 \oplus s_0 = 0 \\ \Longrightarrow\quad & s \in \{000, 101\},\ s \neq 000 \quad \Longrightarrow \quad s = 101. \end{aligned}$$

Preparazione e oracolo

↓

Distribuzione degli esiti

↓

Interpretazione secondo la promessa

La misura di Bernstein–Vazirani ha restituito direttamente i coefficienti della parità. Le misure di Simon hanno invece determinato due condizioni, dalle quali abbiamo ricostruito l'unica stringa non nulla compatibile. In entrambi i casi i calcoli delle ampiezze e delle probabilità spiegano quale informazione otteniamo dalla funzione.

$y^{(1)}, y^{(2)}$ sono due risultati misurati in A. Nella stringa nascosta $s_2 s_1 s_0$, s_2 è il primo bit, s_1 il centrale e s_0 l'ultimo. Parità: 0 per un numero pari di bit 1, 1 per un numero dispari. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Promessa di Simon: ogni uscita ha due ingressi, x e $x \oplus s$, con $s \neq 0^n$.

Appendice: i conti delle altre coppie

Il percorso principale ha già ricostruito le stringhe nascoste e giustificato il procedimento. Qui sono raccolti i calcoli completi che verificano le tabelle di confronto, senza interrompere la sequenza degli esempi.

Esempio 101. Normalizzazione e otto ampiezze per le coppie 001, 100; 010, 111; 011, 110.

Esempio 111. Normalizzazione e otto ampiezze per le coppie 001, 110; 010, 101; 011, 100.

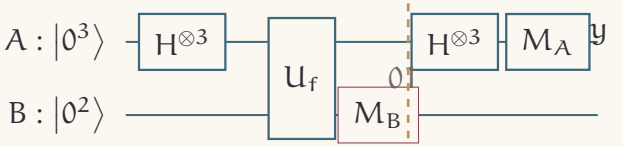
Nuove etichette. Stato congiunto e ampiezze dopo la ricodifica delle uscite di B.

Ogni gruppo riparte dalla coppia selezionata, calcola la normalizzazione e sviluppa le due trasformate complete. La somma evidenzia in rosso le cancellazioni e in blu i contributi che si rafforzano. I collegamenti riportano al confronto nel percorso principale.

Tabelle nel percorso principale: esempio 101, slide 105; esempio 111, slide 121. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri.

La lettura B=01 seleziona 001 e 100

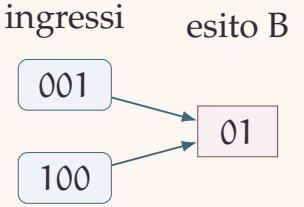
Riprendiamo l'esempio con stringa nascosta $s = 101$. L'uscita $B = 01$ seleziona gli ingressi 001 e 100, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.



Lettura di B: coppia selezionata

$$P(B = 01) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 01)} = \frac{1}{2},$$

$$|\phi_{B=01}\rangle = \frac{(|001\rangle + |100\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|001\rangle + |100\rangle)$$
$$= \frac{|001\rangle + |100\rangle}{\sqrt{2}}.$$



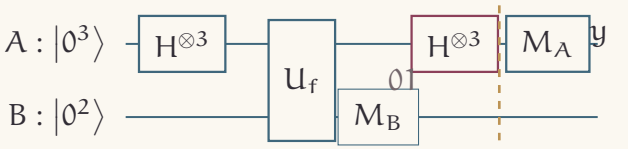
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|001\rangle+|100\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 105. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 001 e 100

Dopo la lettura B = 01, A è nello stato $\frac{|001\rangle+|100\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|001\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle\Big],$$

$$H^{\otimes 3}|100\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle\Big].$$

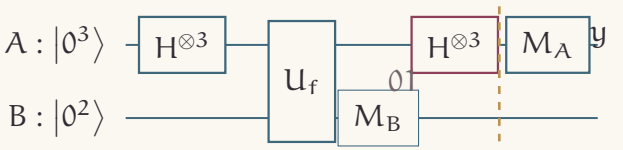
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 001 e 100

Sommiamo le due espansioni di $\frac{|001\rangle+|100\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{8}}=\frac{1}{\sqrt{16}}=\frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|001\rangle+|100\rangle}{\sqrt{2}}$$

$$=\frac{1}{4}\Big[(1+1)|000\rangle+(-1+1)|001\rangle+(1+1)|010\rangle+(-1+1)|011\rangle$$
$$+(1-1)|100\rangle+(-1-1)|101\rangle+(1-1)|110\rangle+(-1-1)|111\rangle\Big]$$

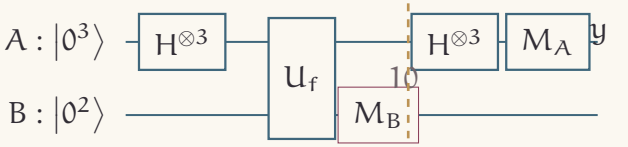
$$=\frac{2|000\rangle+2|010\rangle-2|101\rangle-2|111\rangle}{4}=\frac{|000\rangle+|010\rangle-|101\rangle-|111\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2 = 1/4$, come nel confronto alla slide 105.

A è il registro che misureremo. Qui B ha dato 01. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=10 seleziona 010 e 111

Riprendiamo l'esempio con stringa nascosta $s = 101$. L'uscita $B = 10$ seleziona gli ingressi 010 e 111, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.

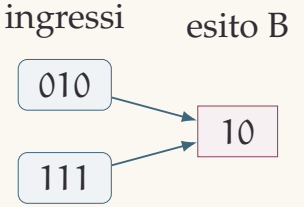


Lettura di B: coppia selezionata

$$P(B = 10) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 10)} = \frac{1}{2},$$

$$|\phi_{B=10}\rangle = \frac{(|010\rangle + |111\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|010\rangle + |111\rangle)$$

$$= \frac{|010\rangle + |111\rangle}{\sqrt{2}}.$$



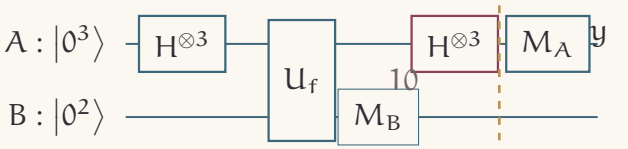
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|010\rangle+|111\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 105. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 010 e 111

Dopo la lettura B = 10, A è nello stato $\frac{|010\rangle+|111\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|010\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle\Big],$$

$$H^{\otimes 3}|111\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle - |010\rangle + |011\rangle - |100\rangle + |101\rangle + |110\rangle - |111\rangle\Big].$$

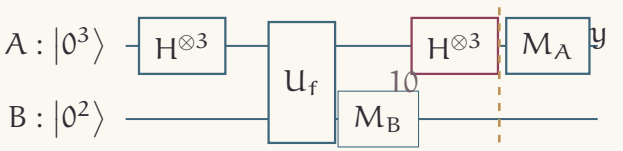
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 010 e 111

Sommiamo le due espansioni di $\frac{|010\rangle+|111\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|010\rangle + |111\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\Big[(1+1)|000\rangle + (1-1)|001\rangle + (-1-1)|010\rangle + (-1+1)|011\rangle + (1-1)|100\rangle + (1+1)|101\rangle + (-1+1)|110\rangle + (-1-1)|111\rangle \Big]$$

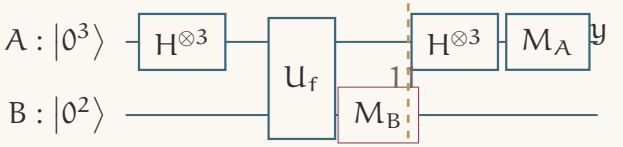
$$= \frac{2|000\rangle - 2|010\rangle + 2|101\rangle - 2|111\rangle}{4} = \frac{|000\rangle - |010\rangle + |101\rangle - |111\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2 = 1/4$, come nel confronto alla slide 105.

A è il registro che misureremo. Qui B ha dato 10. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=11 seleziona 011 e 110

Riprendiamo l'esempio con stringa nascosta $s = 101$. L'uscita $B = 11$ seleziona gli ingressi 011 e 110, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.

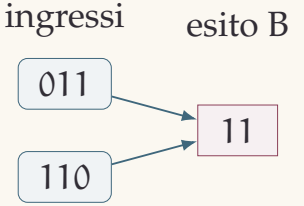


Lettura di B: coppia selezionata

$$P(B = 11) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 11)} = \frac{1}{2},$$

$$|\phi_{B=11}\rangle = \frac{(|011\rangle + |110\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|011\rangle + |110\rangle)$$

$$= \frac{|011\rangle + |110\rangle}{\sqrt{2}}.$$



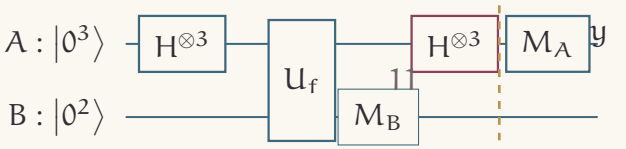
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|011\rangle+|110\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 105. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 011 e 110

Dopo la lettura B = 11, A è nello stato $\frac{|011\rangle+|110\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|011\rangle = \frac{1}{\sqrt{8}}\Big[\,|000\rangle - |001\rangle - |010\rangle + |011\rangle + |100\rangle - |101\rangle - |110\rangle + |111\rangle\,\Big],$$

$$H^{\otimes 3}|110\rangle = \frac{1}{\sqrt{8}}\Big[\,|000\rangle + |001\rangle - |010\rangle - |011\rangle - |100\rangle - |101\rangle + |110\rangle + |111\rangle\,\Big].$$

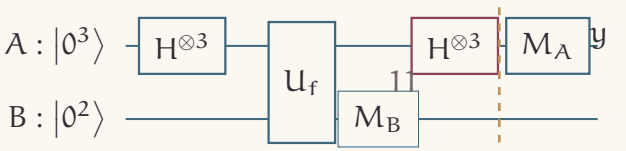
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 011 e 110

Sommiamo le due espansioni di $\frac{|011\rangle+|110\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|011\rangle + |110\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\left[\begin{array}{llll} (1+1)|000\rangle & + (-1+1)|001\rangle & + (-1-1)|010\rangle & + (1-1)|011\rangle \\ + (1-1)|100\rangle & + (-1-1)|101\rangle & + (-1+1)|110\rangle & + (1+1)|111\rangle \end{array}\right]$$

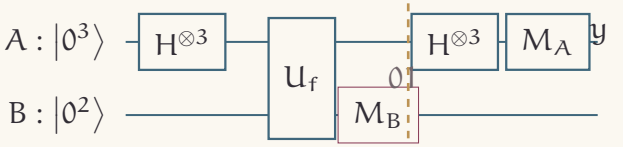
$$= \frac{2|000\rangle - 2|010\rangle - 2|101\rangle + 2|111\rangle}{4} = \frac{|000\rangle - |010\rangle - |101\rangle + |111\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2 = 1/4$, come nel confronto alla slide 105.

A è il registro che misureremo. Qui B ha dato 11. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=01 seleziona 001 e 110

Riprendiamo l'esempio con stringa nascosta $s = 111$. L'uscita $B = 01$ seleziona gli ingressi 001 e 110, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.

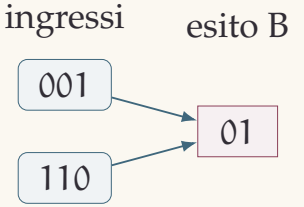


Lettura di B: coppia selezionata

$$P(B = 01) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 01)} = \frac{1}{2},$$

$$|\phi_{B=01}\rangle = \frac{(|001\rangle + |110\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|001\rangle + |110\rangle)$$

$$= \frac{|001\rangle + |110\rangle}{\sqrt{2}}.$$



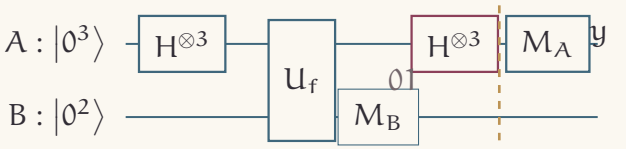
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|001\rangle+|110\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 121. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 001 e 110

Dopo la lettura B = 01, A è nello stato $\frac{|001\rangle+|110\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|001\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle + |110\rangle - |111\rangle\Big],$$

$$H^{\otimes 3}|110\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle - |010\rangle - |011\rangle - |100\rangle - |101\rangle + |110\rangle + |111\rangle\Big].$$

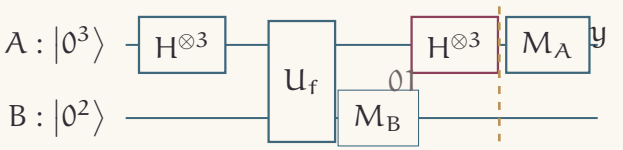
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 001 e 110

Sommiamo le due espansioni di $\frac{|001\rangle+|110\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|001\rangle + |110\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\left[\begin{array}{l} (1+1)\,|000\rangle + (-1+1)\,|001\rangle + (1-1)\,|010\rangle + (-1-1)\,|011\rangle \\ + (1-1)\,|100\rangle + (-1-1)\,|101\rangle + (1+1)\,|110\rangle + (-1+1)\,|111\rangle \end{array}\right]$$

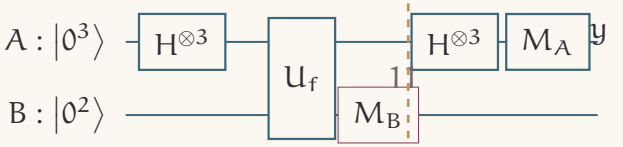
$$= \frac{2\,|000\rangle - 2\,|011\rangle - 2\,|101\rangle + 2\,|110\rangle}{4} = \frac{|000\rangle - |011\rangle - |101\rangle + |110\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2 = 1/4$, come nel confronto alla slide 121.

A è il registro che misureremo. Qui B ha dato 01. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=11 seleziona 010 e 101

Riprendiamo l'esempio con stringa nascosta $s = 111$. L'uscita $B = 11$ seleziona gli ingressi 010 e 101, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.

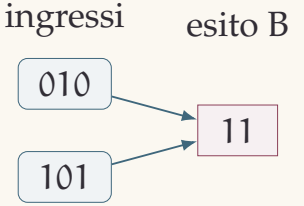


Lettura di B: coppia selezionata

$$P(B = 11) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 11)} = \frac{1}{2},$$

$$|\phi_{B=11}\rangle = \frac{(|010\rangle + |101\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|010\rangle + |101\rangle)$$

$$= \frac{|010\rangle + |101\rangle}{\sqrt{2}}.$$



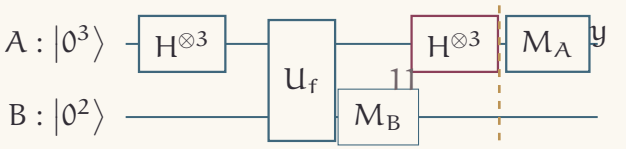
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|010\rangle+|101\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 121. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 010 e 101

Dopo la lettura B = 11, A è nello stato $\frac{|010\rangle+|101\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|010\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle - |010\rangle - |011\rangle + |100\rangle + |101\rangle - |110\rangle - |111\rangle\Big],$$

$$H^{\otimes 3}|101\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle + |010\rangle - |011\rangle - |100\rangle + |101\rangle - |110\rangle + |111\rangle\Big].$$

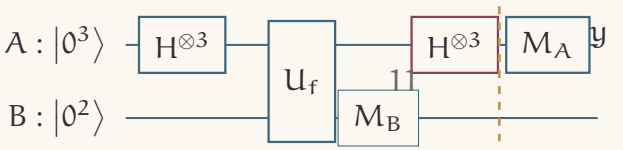
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 010 e 101

Sommiamo le due espansioni di $\frac{|010\rangle+|101\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{8}}=\frac{1}{\sqrt{16}}=\frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|010\rangle+|101\rangle}{\sqrt{2}}$$

$$=\frac{1}{4}\Big[(1+1)|000\rangle+(1-1)|001\rangle+(-1+1)|010\rangle+(-1-1)|011\rangle$$
$$+(1-1)|100\rangle+(1+1)|101\rangle+(-1-1)|110\rangle+(-1+1)|111\rangle\Big]$$

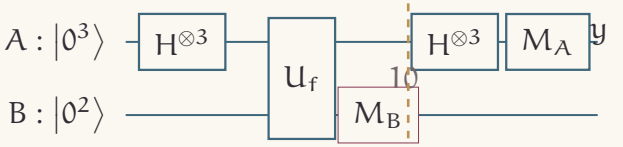
$$=\frac{2|000\rangle-2|011\rangle+2|101\rangle-2|110\rangle}{4}=\frac{|000\rangle-|011\rangle+|101\rangle-|110\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2=1/4$, come nel confronto alla slide 121.

A è il registro che misureremo. Qui B ha dato 11. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

La lettura B=10 seleziona 011 e 100

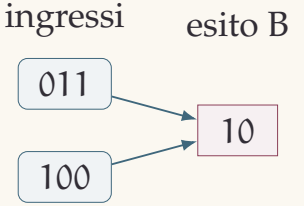
Riprendiamo l'esempio con stringa nascosta $s = 111$. L'uscita $B = 10$ seleziona gli ingressi 011 e 100, ciascuno con ampiezza $1/\sqrt{8}$. Calcoliamo la probabilità di questa uscita e normalizziamo lo stato di A.



Lettura di B: coppia selezionata

$$P(B = 10) = 2\left|\frac{1}{\sqrt{8}}\right|^2 = \frac{2}{8} = \frac{1}{4}, \qquad \sqrt{P(B = 10)} = \frac{1}{2},$$

$$|\phi_{B=10}\rangle = \frac{(|011\rangle + |100\rangle)/\sqrt{8}}{1/2} = \frac{2}{\sqrt{8}}(|011\rangle + |100\rangle)$$
$$= \frac{|011\rangle + |100\rangle}{\sqrt{2}}.$$



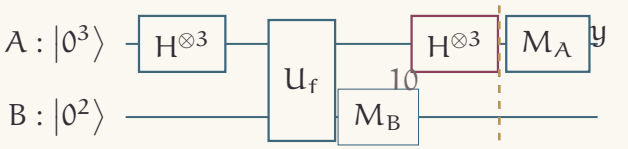
L'esito di B seleziona la coppia di ingressi.

La lettura di B lascia A nello stato $\frac{|011\rangle+|100\rangle}{\sqrt{2}}$. Calcoliamo le due trasformate complete e poi sommiamo i contributi allo stesso ket finale.

Questi conti verificano la tabella di confronto alla slide 121. A contiene tre qubit; B contiene l'etichetta di due bit della coppia. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Normalizzare: dividere per la norma, radice della somma dei moduli quadri. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le Hadamard sui due termini 011 e 100

Dopo la lettura B = 10, A è nello stato $\frac{|011\rangle+|100\rangle}{\sqrt{2}}$. Trasformiamo separatamente i due ket. I contributi allo stesso ket finale sono allineati nelle due espansioni:



Dopo le Hadamard finali

$$H^{\otimes 3}|011\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle - |001\rangle - |010\rangle + |011\rangle + |100\rangle - |101\rangle - |110\rangle + |111\rangle \Big],$$

$$H^{\otimes 3}|100\rangle = \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle - |100\rangle - |101\rangle - |110\rangle - |111\rangle \Big].$$

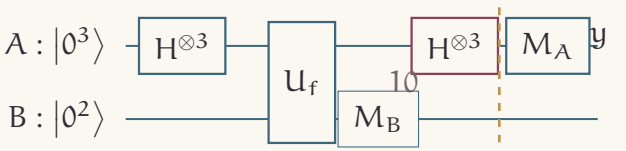
Ogni trasformata ha otto termini. Sommiamole con il fattore iniziale $1/\sqrt{2}$: i contributi rossi si cancelleranno, quelli blu si sommeranno.

$H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Tre Hadamard danno il fattore $(1/\sqrt{2})^3 = 1/\sqrt{8}$. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Sommiamo le trasformate di 011 e 100

Sommiamo le due espansioni di $\frac{|011\rangle+|100\rangle}{\sqrt{2}}$. Il fattore comune è:

$$\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{8}} = \frac{1}{\sqrt{16}} = \frac{1}{4}.$$



Dopo le Hadamard finali

$$H^{\otimes 3}\frac{|011\rangle + |100\rangle}{\sqrt{2}}$$

$$= \frac{1}{4}\Big[(1+1)\,|000\rangle + (-1+1)\,|001\rangle + (-1+1)\,|010\rangle + (1+1)\,|011\rangle + (1-1)\,|100\rangle + (-1-1)\,|101\rangle + (-1-1)\,|110\rangle + (1-1)\,|111\rangle\Big]$$

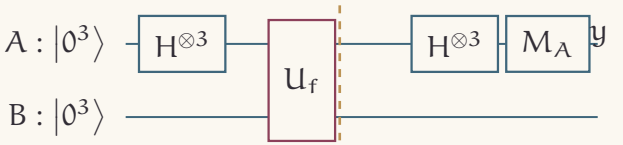
$$= \frac{2\,|000\rangle + 2\,|011\rangle - 2\,|101\rangle - 2\,|110\rangle}{4} = \frac{|000\rangle + |011\rangle - |101\rangle - |110\rangle}{2}.$$

Ciascuno dei quattro ket rimasti ha probabilità $|\pm 1/2|^2 = 1/4$, come nel confronto alla slide 121.

A è il registro che misureremo. Qui B ha dato 10. Cerchi rossi: contributi opposti, somma zero. Cerchi blu: contributi con lo stesso segno, somma $+2$ oppure -2. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Lo stato congiunto dopo la rietichettatura

Riprendiamo la ricodifica delle slide 126–127, con $s = 101$. Le etichette $00, 01, 10, 11$ diventano $000, 001, 010, 100$. A e B contengono tre qubit ciascuno. Scriviamo lo stato dopo il nuovo oracolo.



Dopo l'oracolo

$$U_{f'}\,|x, 000\rangle = |x, 000 \oplus g(f(x))\rangle = |x, g(f(x))\rangle\,,$$

$$U_{f'}\,\frac{1}{\sqrt{8}}\sum_x |x, 000\rangle = \frac{1}{\sqrt{8}}\sum_x |x, g(f(x))\rangle\,.$$

$$|\Psi_{\text{inizio}}\rangle = |000\rangle\,|000\rangle\,, \quad \left|\Psi_{\text{prep}}\right\rangle = \frac{1}{\sqrt{8}}\sum_x |x, 000\rangle\,,$$

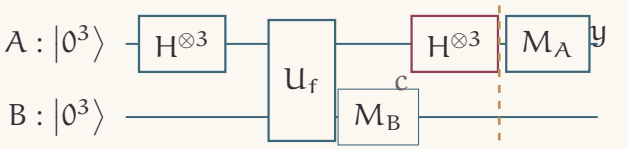
$$\begin{aligned}|\Psi'_{\text{oracolo}}\rangle = \frac{1}{\sqrt{8}}(&|000, 000\rangle + |001, 001\rangle + |010, 010\rangle + |011, 100\rangle \\ &+ |100, 001\rangle + |101, 000\rangle + |110, 100\rangle + |111, 010\rangle).\end{aligned}$$

Ogni etichetta ha probabilità $2(1/\sqrt{8})^2 = 1/4$. Dividendo per $\sqrt{1/4} = 1/2$, le ampiezze selezionate diventano $(1/\sqrt{8})/(1/2) = 1/\sqrt{2}$. Ritroviamo le coppie già trasformate.

$f' = g \circ f$ cambia le etichette. In $|x, c\rangle$, x è in A e c in B. XOR ($\oplus$): somma dei bit modulo 2, quindi $1 \oplus 1 = 0$. Oracolo: operazione che rende disponibile la funzione f. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.

Le ampiezze conservate dalla nuova codifica

Le nuove etichette di B selezionano le stesse coppie. Le due espansioni e la loro somma restano identiche: raccogliamo gli stati finali, con tutti i ket e i loro segni.



Dopo le Hadamard finali

$$\mathrm{B} = 000: \quad \mathrm{H}^{\otimes 3}\frac{|000\rangle + |101\rangle}{\sqrt{2}} = \frac{|000\rangle + |010\rangle + |101\rangle + |111\rangle}{2},$$

$$\mathrm{B} = 001: \quad \mathrm{H}^{\otimes 3}\frac{|001\rangle + |100\rangle}{\sqrt{2}} = \frac{|000\rangle + |010\rangle - |101\rangle - |111\rangle}{2},$$

$$\mathrm{B} = 010: \quad \mathrm{H}^{\otimes 3}\frac{|010\rangle + |111\rangle}{\sqrt{2}} = \frac{|000\rangle - |010\rangle + |101\rangle - |111\rangle}{2},$$

$$\mathrm{B} = 100: \quad \mathrm{H}^{\otimes 3}\frac{|011\rangle + |110\rangle}{\sqrt{2}} = \frac{|000\rangle - |010\rangle - |101\rangle + |111\rangle}{2}.$$

Le altre quattro componenti si sono cancellate. Ogni ampiezza rimasta vale $+1/2$ o $-1/2$, quindi ogni risultato ammesso ha probabilità $1/4$. La distribuzione di A resta uguale.

I conti completi sono alle slide 102–103, 161–162, 164–165 e 167–168. Ampiezza: coefficiente dello stato. Per un coefficiente reale a, $p = |a|^2 = a^2$. Il ket $|x\rangle$ indica lo stato di base associato alla stringa x.