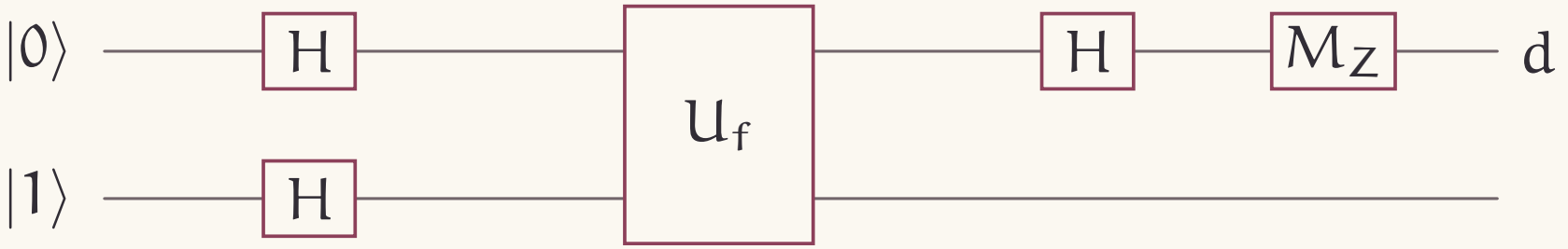
Circuiti quantistici

Da Deutsch a Deutsch–Jozsa



Porte, interferenza e logica reversibile

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 14 ottobre 2026. Scelta degli esempi, oracoli espliciti e percorso narrativo consolidato.

Percorso del modulo

Le porte e la logica reversibile conducono al circuito di Deutsch. La sua estensione a più bit mantiene registri, preparazione e lettura per interferenza, rendendo esplicito il confronto dei costi. Gli esempi a due e tre bit sono svolti lungo la derivazione; dimostrazioni complementari e varianti sono raccolte dopo il percorso principale.

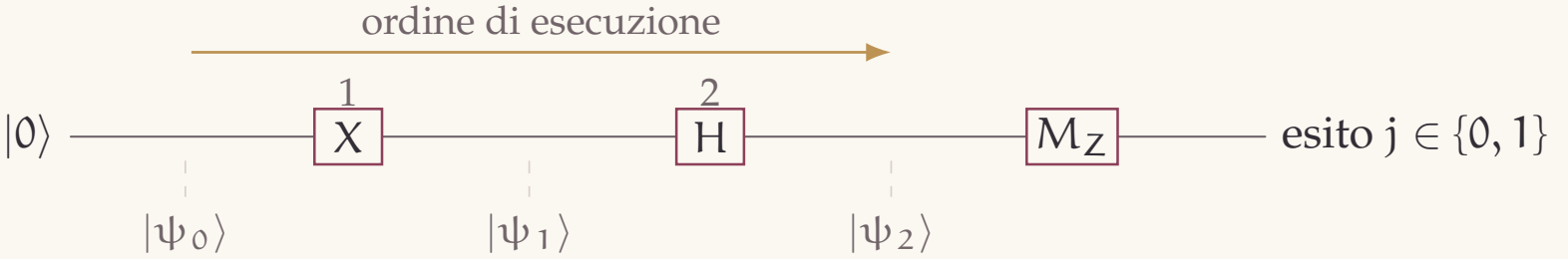
1. Lettura ed esecuzione
2. Porte a un qubit
3. Composizione e inversione
4. Fasi e interferenza
5. Registri di due qubit
6. CNOT, Toffoli e ausiliari
7. Deutsch: derivazione commentata
8. Interpretazione e prosecuzione
9. Deutsch–Jozsa su più bit
A. Verifiche e dimostrazioni
B. Preparazioni alternative
C. AND, fase e ripristino

I circuiti identificano la trasformazione corrente; formule e dati locali permettono di seguire lo stesso stato da una slide alla successiva.

$f : \{0,1\}^n \to \{0,1\}$; n: bit dell'ingresso. Una funzione costante ha sempre lo stesso valore; una bilanciata ha uguale numero di zeri e uni. Il caso $n = 1$ è Deutsch, il caso generale è Deutsch–Jozsa.

Leggere ed eseguire il primo circuito

Seguiamo l'esecuzione di un circuito: prepariamo $|0\rangle$, applichiamo X e poi H, infine misuriamo nella base $(|0\rangle, |1\rangle)$. Il tempo procede da sinistra a destra nel disegno.



$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = X|\psi_0\rangle, \quad |\psi_2\rangle = H|\psi_1\rangle = HX|0\rangle.$$

La matrice più vicina al vettore agisce per prima. Per una sequenza U_1, U_2, U_3, l'uscita è $U_3U_2U_1|\psi_0\rangle$.
Calcoleremo le probabilità degli esiti 0 e 1; ogni esecuzione produce un solo esito.

La scrittura $HX|0\rangle$ traduce il circuito in un prodotto di matrici. Per eseguirlo dobbiamo rappresentare lo stato mediante le sue ampiezze.

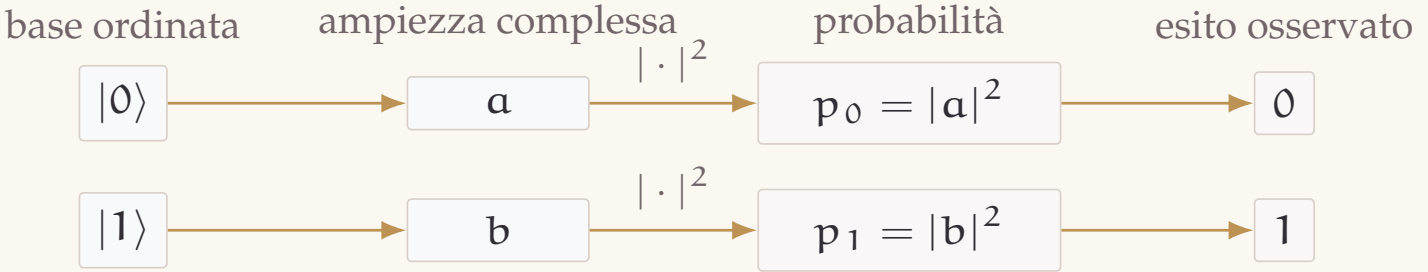
BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. M_Z misura nella base $(|0\rangle, |1\rangle)$: $p_0 = |a|^2$, $p_1 = |b|^2$. ψ_k: stato dopo k porte; U_k: porta applicata al passo k.

Il vettore usato dal simulatore

Nella base ordinata $(|0\rangle, |1\rangle)$, il simulatore conserva le ampiezze complesse nella colonna $(a, b)^{\mathsf{T}}$: la prima componente accompagna $|0\rangle$, la seconda $|1\rangle$.

$$|\psi\rangle = a|0\rangle + b|1\rangle \longleftrightarrow \begin{pmatrix} a \\ b \end{pmatrix}, \qquad |a|^2 + |b|^2 = 1.$$

Per $|0\rangle = (1, 0)^{\mathsf{T}}$ si ha $|1|^2 + |0|^2 = 1 + 0 = 1$.
Il vettore ha dimensione 2×1. Ogni preparazione e misura produce un esito; le ripetizioni danno conteggi.



Le ampiezze costituiscono i dati del calcolo. La misura ne ricava probabilità attraverso i moduli quadri; conserveremo quindi i coefficienti complessi durante tutta l'esecuzione.

DATI LOCALI $|0\rangle = (1, 0)^{\mathsf{T}}$, $|1\rangle = (0, 1)^{\mathsf{T}}$; $a, b \in \mathbb{C}$, $|z|^2 = z^* z$. T trasforma la riga (a, b) nella colonna $(a, b)^{\mathsf{T}}$.

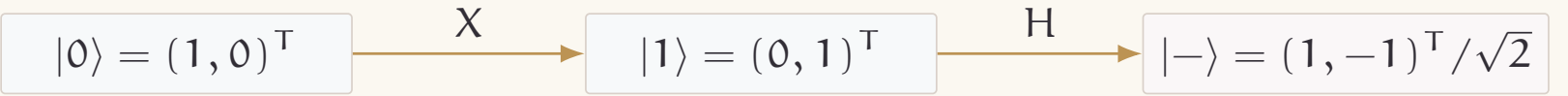
Eseguire X e poi H

Con $|0\rangle = (1,0)^{\mathsf{T}}$, eseguiamo il programma $HX|0\rangle$ nell'ordine indicato dal circuito. Il primo prodotto fornisce lo stato intermedio; il secondo usa quel risultato come ingresso. La norma finale controlla la normalizzazione.

$$X|0\rangle = \begin{pmatrix} 0\cdot 1 + 1\cdot 0 \\ 1\cdot 1 + 0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle.$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 0 + 1\cdot 1 \\ 1\cdot 0 - 1\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle.$$

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



L'uscita è $|-\rangle = (1,-1)^{\mathsf{T}}/\sqrt{2}$. Il segno appartiene all'ampiezza: per prevedere gli esiti dobbiamo applicare la regola di Born allo stato appena ottenuto.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^{\mathsf{T}}/\sqrt{2}$. $\|(a,b)^{\mathsf{T}}\|^2 = |a|^2 + |b|^2$; $|z|^2 = z^* z$.

Probabilità e stati dopo la misura

Per $|\psi\rangle = (a, b)^T$, la misura seleziona il ramo $v_0 = (a, 0)^T$ oppure $v_1 = (0, b)^T$. Assumiamo $p_j = \|v_j\|^2$ e $|\psi_j\rangle = v_j/\sqrt{p_j}$ per $p_j > 0$. L'ingresso $|-\rangle = (1, -1)^T/\sqrt{2}$ ha $a = 1/\sqrt{2}$, $b = -1/\sqrt{2}$.

ramo 0	peso	stato dopo l'esito 0
v_0	$p_0 = \|v_0\|^2$	$\|\psi_0\rangle = v_0/\sqrt{p_0}$

$$v_0 = (1, 0)^T/\sqrt{2},$$
$$p_0 = |1/\sqrt{2}|^2 = 1/2,$$
$$\frac{v_0}{\sqrt{p_0}} = \frac{1/\sqrt{2}}{1/\sqrt{2}}(1, 0)^T = (1, 0)^T = |0\rangle.$$

ramo 1	peso	stato dopo l'esito 1
v_1	$p_1 = \|v_1\|^2$	$\|\psi_1\rangle = v_1/\sqrt{p_1}$

$$v_1 = (0, -1)^T/\sqrt{2},$$
$$p_1 = |-1/\sqrt{2}|^2 = (-1)(-1)/2 = 1/2,$$
$$\frac{v_1}{\sqrt{p_1}} = \frac{1/\sqrt{2}}{1/\sqrt{2}}(0, -1)^T = (0, -1)^T = -|1\rangle.$$

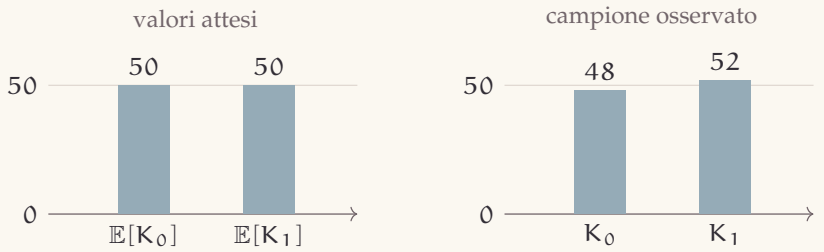
Le alternative hanno peso totale $p_0 + p_1 = 1/2 + 1/2 = 1$. Dopo aver osservato 1, una seconda misura M_Z immediata dà $p(1 \mid \text{primo esito } 1) = |-1|^2 = 1$.

La normalizzazione descrive lo stato del ramo osservato. Il segno comune di $-|1\rangle$ è una fase globale e conserva i pesi della misura; un nuovo campione della distribuzione iniziale richiede invece una nuova preparazione di $|-\rangle$.

DATI LOCALI $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $\|(x, y)^T\|^2 = |x|^2 + |y|^2$, $|z|^2 = z^*z$. v_j: proiezione; p_j: peso; $|\psi_j\rangle$: stato condizionato. La divisione richiede $p_j > 0$.

Dalle probabilità ai conteggi

Il circuito $|0\rangle \to X \to H \to M_Z$ dà $p_0 = p_1 = 1/2$. Consideriamo $N = 100$ esecuzioni indipendenti, ciascuna con una nuova preparazione: i conteggi medi e un campione osservato si confrontano sulla stessa scala.



Ogni barra conta esiti in cento esecuzioni.

$$\mathbb{E}[K_0] = 100 \cdot \frac{1}{2} = 50, \qquad \mathbb{E}[K_1] = 100 \cdot \frac{1}{2} = 50.$$

Per $K_0 = 48$, $K_1 = 52$:

$$\widehat{p}_0 = \frac{48}{100} = 0{,}48, \qquad \widehat{p}_1 = \frac{52}{100} = 0{,}52,$$

$$0{,}48 + 0{,}52 = 1.$$

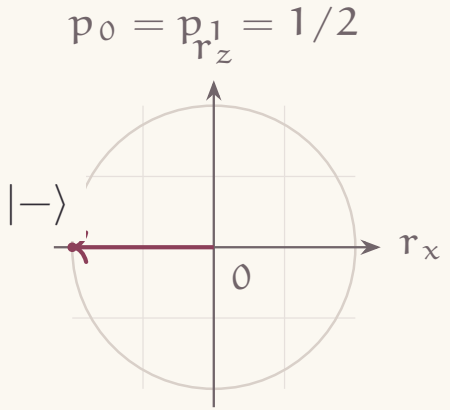
I conteggi variano fra campioni; il valore atteso è la media su ripetizioni dell'intero esperimento.

I conteggi stimano i moduli quadri; le coordinate geometriche permetteranno di distinguere anche stati con identici conteggi attesi e fasi relative diverse.

$|0\rangle = (1,0)^T$, $|-\rangle = (1,-1)^T/\sqrt{2}$; $X(a,b)^T = (b,a)^T$. $H(a,b)^T = (a+b, a-b)^T/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. M_Z indica la misura nella base $(|0\rangle, |1\rangle)$. K_j: conteggio; $\widehat{p}_j = K_j/N$: frequenza; si assume $\mathbb{E}[K_j] = N p_j$, con $N = 100$.

Le coordinate geometriche di uno stato

Per lo stato puro normalizzato $|\psi\rangle = a|0\rangle + b|1\rangle$, i moduli quadri determinano la quota. Il prodotto $q = a^* b$, che dipende dai moduli e dalla fase relativa, determina le due coordinate orizzontali.



$$r = (-1, 0, 0), \quad r_y = 0$$

Il punto illustrato è quello dell'esempio $|-\rangle$.

$$\underbrace{|a|^2}_{p_0}, \underbrace{|b|^2}_{p_1} \longrightarrow r_z = p_0 - p_1.$$

$$q = \underbrace{\operatorname{Re} q}_{\text{parte reale}} + i \underbrace{\operatorname{Im} q}_{\text{parte immaginaria}} \longrightarrow \begin{cases} r_x = 2 \operatorname{Re} q, \\ r_y = 2 \operatorname{Im} q. \end{cases}$$

Per $|-\rangle = (1, -1)^T/\sqrt{2}$:

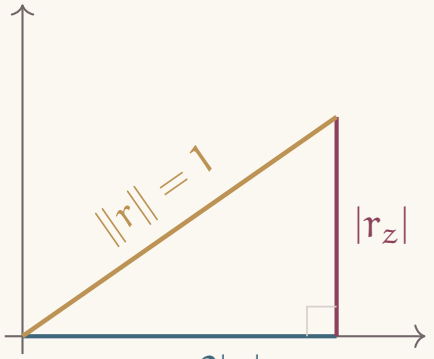
$$q = (1/\sqrt{2})(-1/\sqrt{2}) = -1/2,$$
$$r_x = 2(-1/2) = -1, \quad r_y = 2 \cdot 0 = 0,$$
$$r_z = 1/2 - 1/2 = 0, \qquad r = (-1, 0, 0).$$

La quota r_z confronta le probabilità dei due esiti; le coordinate orizzontali dipendono dalla relazione fra le ampiezze. Verifichiamo ora perché il punto appartenga a una sfera.

BASE $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $(a, b)^T = a|0\rangle + b|1\rangle$. $|a|^2 + |b|^2 = 1$, $|z|^2 = z^* z$; a^* è il coniugato. $(a, b)^T \in \mathbb{C}^2$ contiene ampiezze; $r \in \mathbb{R}^3$ contiene coordinate geometriche.

La normalizzazione determina la sfera

Per verificare il raggio della rappresentazione, ripartiamo da $q = a^* b$, $p_0 = |a|^2$, $p_1 = |b|^2$ e $p_0 + p_1 = 1$. La distanza dall'origine combina la componente orizzontale $r_\perp$ e la quota r_z.



Cateti: $r_\perp$ e $|r_z|$.

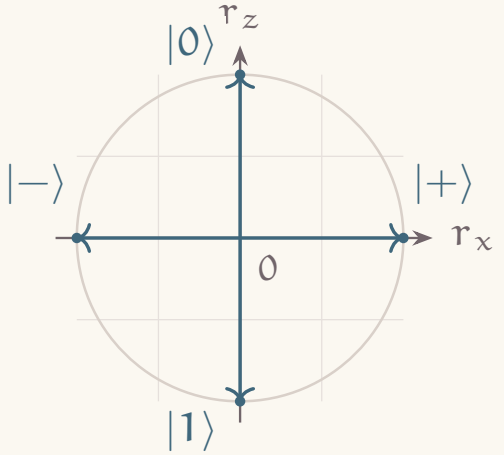
$$
\begin{aligned}
r_\perp^2 = r_x^2 + r_y^2 &= 4[(\operatorname{Re} q)^2 + (\operatorname{Im} q)^2] = 4|q|^2 \\
&= 4(a^* b)^*(a^* b) = 4(a b^*)(a^* b) \\
&= 4(a a^*)(b^* b) = 4 p_0 p_1, \\
r_x^2 + r_y^2 + r_z^2 &= 4 p_0 p_1 + (p_0 - p_1)^2 \\
&= 4 p_0 p_1 + p_0^2 - 2 p_0 p_1 + p_1^2 \\
&= p_0^2 + 2 p_0 p_1 + p_1^2 \\
&= (p_0 + p_1)^2 = 1^2 = 1.
\end{aligned}
$$

La normalizzazione dello stato puro impone $\|r\| = 1$. Il cateto verticale ha lunghezza $|r_z|$, mentre la quota conserva il segno di $p_0 - p_1$; poiché il disegno è proiettato sul foglio, una freccia può apparire più corta.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $r_x = 2\operatorname{Re}(a^* b)$, $r_y = 2\operatorname{Im}(a^* b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $|q|^2 = (\operatorname{Re} q)^2 + (\operatorname{Im} q)^2 = q^* q$; $(a^* b)^* = a b^*$; $a a^* = |a|^2$, $b^* b = |b|^2$; $r_\perp = \sqrt{r_x^2 + r_y^2} = 2|q|$. $\|r\|^2 = r_x^2 + r_y^2 + r_z^2$.

Quattro stati di riferimento sulla sfera

Fissiamo quattro riferimenti per leggere le figure successive: $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$, $|\pm\rangle = (1,\pm1)^{\mathsf{T}}/\sqrt{2}$. Le ampiezze reali danno $\mathrm{Im}(a^*b) = 0$, quindi tutti i punti appartengono alla sezione $r_y = 0$.



Sezione $r_y = 0$ nel piano (r_x, r_z).

$$|0\rangle:\ a^*b = 1\cdot 0 = 0, \quad r = (0,0,1^2-0^2) = (0,0,1);$$
$$|1\rangle:\ a^*b = 0\cdot 1 = 0, \quad r = (0,0,0^2-1^2) = (0,0,-1).$$
$$|\pm\rangle:\ a^*b = \frac{1}{\sqrt{2}}\frac{\pm 1}{\sqrt{2}} = \pm\frac{1}{2},$$
$$r_x = 2(\pm 1/2) = \pm 1, \quad r_z = 1/2 - 1/2 = 0.$$

I poli danno rispettivamente $p_0 = 1$, $p_1 = 1$. All'equatore $p_0 = p_1 = (1/\sqrt{2})^2 = 1/2$.

I poli rappresentano esiti certi. I due punti equatoriali hanno probabilità uguali e segni relativi diversi: questa differenza sarà resa osservabile mediante Hadamard.

$|\psi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$; Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^*z$.

Le tre porte impiegate nel percorso

Confrontiamo X, Z e H nella stessa base $(|0\rangle, |1\rangle)$. Le matrici realizzano rispettivamente lo scambio delle ampiezze, il cambio di segno della seconda e la ricombinazione in somma e differenza.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

$(a, b)^\top \xrightarrow{X} (b, a)^\top$ $\quad$ $(a, b)^\top \xrightarrow{Z} (a, -b)^\top$ $\quad$ $(a, b)^\top \xrightarrow{H} (a + b, a - b)^\top/\sqrt{2}$

$$\begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} u_{00}a + u_{01}b \\ u_{10}a + u_{11}b \end{pmatrix}.$$

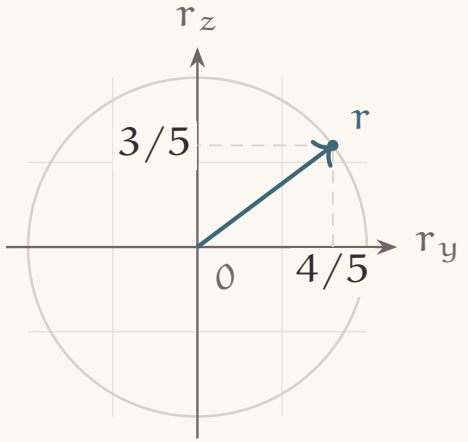
Il prodotto ha dimensioni $(2 \times 2)(2 \times 1) = (2 \times 1)$; la riga j determina la componente d'uscita j, mentre la colonna k si riferisce alla componente d'ingresso k.

Per confrontare le porte useremo lo stesso stato con ampiezze complesse. La coppia vettore e figura permetterà di riconoscere quali proprietà cambiano sotto ciascuna operazione.

BASE $|0\rangle = (1, 0)^\top$, $|1\rangle = (0, 1)^\top$; $(a, b)^\top = a|0\rangle + b|1\rangle$. $a, b \in \mathbb{C}$; $j, k \in \{0, 1\}$. u_{jk} è l'elemento alla riga j e alla colonna k; moltiplica l'ampiezza d'ingresso k nel calcolo della componente d'uscita j.

Lo stato numerico di riferimento sulla sfera

Scegliamo $|\psi\rangle = (2, i)^T/\sqrt{5}$ come ingresso comune: le ampiezze hanno moduli diversi e una fase relativa complessa. Queste caratteristiche rendono distinguibili gli effetti di X, Z e H. Prima di applicarle, verifichiamo la norma e localizziamo il punto sulla sfera.



$$\begin{aligned}
\||\psi\rangle\|^2 &= (2^2 + (-i)i)/5 \\
&= (4 - i^2)/5 = (4+1)/5 = 1, \\
a^*b &= (2/\sqrt{5})(i/\sqrt{5}) = 2i/5, \\
r_x &= 2\cdot 0 = 0, \quad r_y = 2\cdot(2/5) = 4/5, \\
r_z &= 4/5 - 1/5 = 3/5, \\
\|r\|^2 &= 0 + 16/25 + 9/25 = 1.
\end{aligned}$$

$a = 2/\sqrt{5}$, $b = i/\sqrt{5}$; sezione $r_x = 0$.

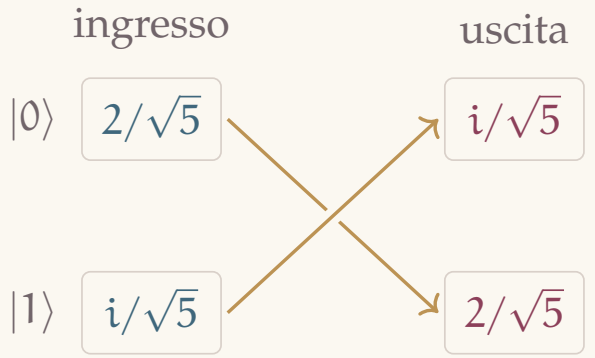
Il punto $r = (0, 4/5, 3/5)$ ha quota positiva: $p_0 = 4/5 > p_1 = 1/5$.

Il punto $r = (0, 4/5, 3/5)$ e il vettore $(2, i)^T/\sqrt{5}$ descrivono lo stesso ingresso. Ripartiremo da questi dati per ciascun confronto.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^*z$. $i^2 = -1$, $i^* = -i$; * indica il coniugato.

Applicare X a uno stato complesso

Applichiamo X a $|\psi\rangle = (2, i)^{\mathsf{T}}/\sqrt{5}$. Ogni riga della matrice seleziona una componente del vettore, producendo lo scambio delle ampiezze. Il prodotto per il coniugato consente di controllare che tale scambio conservi la norma.



Righe: componenti di $|0\rangle$ e $|1\rangle$. In uscita $a' = b$, $b' = a$.

$$\||\psi\rangle\|^2 = \frac{2^2 + (-i)i}{5} = \frac{4+1}{5} = 1.$$

$$X|\psi\rangle = \frac{1}{\sqrt{5}}\begin{pmatrix} 0\cdot 2 + 1\cdot i \\ 1\cdot 2 + 0\cdot i \end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix} i \\ 2 \end{pmatrix}.$$

$$\|X|\psi\rangle\|^2 = \frac{(-i)i + 2^2}{5} = \frac{1+4}{5} = 1.$$

Le due ampiezze vengono scambiate conservando i loro valori complessi.

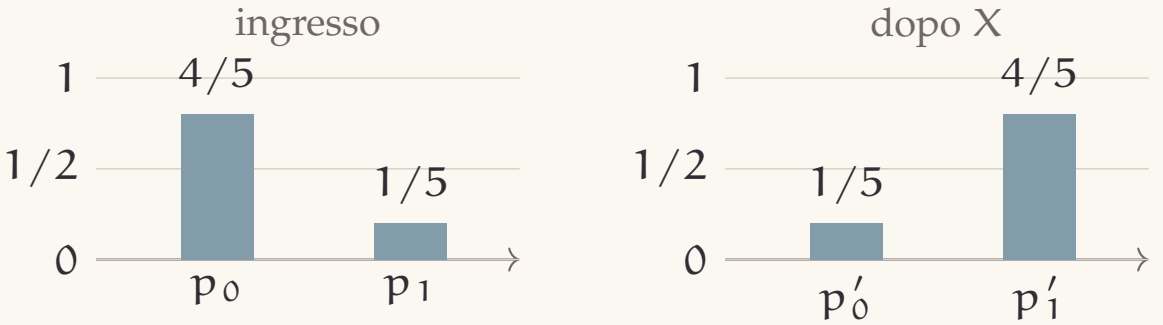
Le due ampiezze cambiano posizione senza cambiare modulo. La distribuzione di misura permetterà di leggere lo stesso scambio nei pesi assegnati agli esiti.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $\|(a,b)^{\mathsf{T}}\|^2 = |a|^2 + |b|^2$; $|z|^2 = z^* z$.

Leggere l'effetto dello scambio

La porta X ha trasformato $(2, i)^{\mathsf{T}}/\sqrt{5}$ in $(i, 2)^{\mathsf{T}}/\sqrt{5}$. Confrontiamo le probabilità prima e dopo l'operazione: ciascun esito riceve il modulo quadro dell'ampiezza che occupa la sua posizione.

$$p_0 = \frac{2^2}{5} = \frac{4}{5}, \quad p_1 = \frac{(-i)i}{5} = \frac{1}{5}; \qquad p_0' = \frac{(-i)i}{5} = \frac{1}{5}, \quad p_1' = \frac{2^2}{5} = \frac{4}{5}.$$



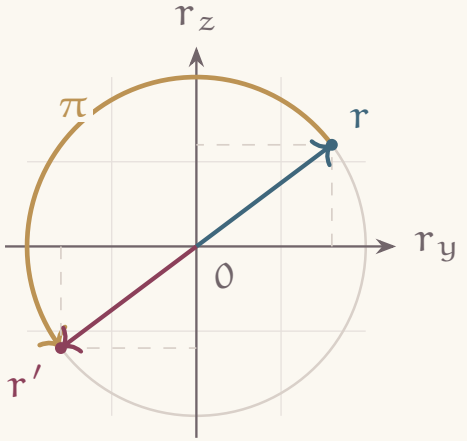
In entrambe le distribuzioni $(4 + 1)/5 = 1$. L'indice identifica l'esito; l'apice indica il peso dopo X.

Le barre scambiano altezza: l'esito più probabile passa da zero a uno. Sulla sfera, questo cambiamento corrisponde all'inversione della quota.

BASE $|0\rangle = (1, 0)^{\mathsf{T}}$, $|1\rangle = (0, 1)^{\mathsf{T}}$; $(a, b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. p_j è il peso prima della porta, p_j' quello dopo la porta.

La geometria dello scambio X

Il risultato $X(2,i)^{\mathsf{T}}/\sqrt{5} = (i,2)^{\mathsf{T}}/\sqrt{5}$ suggerisce un'inversione della quota. Ricaviamo l'intera mappa geometrica per un ingresso generale: poniamo $q = a^* b = q_R + i q_I$, con $q_R, q_I \in \mathbb{R}$, quindi sostituiamo $a' = b$, $b' = a$ nelle coordinate.



Sezione $r_x = 0$; rotazione di π attorno all'asse x.

$$
\begin{aligned}
a'^* b' &= b^* a = q^*, \\
r'_x &= 2\,\mathrm{Re}(q^*) = 2\,\mathrm{Re}(q) = r_x, \\
r'_y &= 2\,\mathrm{Im}(q^*) = -2\,\mathrm{Im}(q) = -r_y, \\
r'_z &= |b|^2 - |a|^2 = -(|a|^2 - |b|^2) = -r_z.
\end{aligned}
$$

Per $r = (0, 4/5, 3/5)$ si ottiene

$$r' = (0, -4/5, -3/5).$$

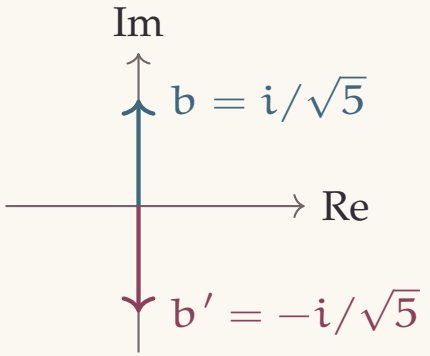
L'asse r_x resta fisso; le altre coordinate cambiano segno. La mappa è una rotazione di π attorno a r_x.

La mappa conserva r_x e inverte r_y, r_z: il punto compie una rotazione di π attorno all'asse x. L'esempio numerico verifica la trasformazione appena ricavata.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^* b)$, $r_y = 2\,\mathrm{Im}(a^* b)$, $r_z = |a|^2 - |b|^2$; Re, Im indicano parte reale e immaginaria. $q = q_R + i q_I$, $q^* = q_R - i q_I$: $\mathrm{Re}\, q^* = \mathrm{Re}\, q$, $\mathrm{Im}\, q^* = -\mathrm{Im}\, q$. $i^2 = -1$, $i^* = -i$; * indica il coniugato.

Applicare Z allo stesso ingresso

Ripartiamo dallo stesso ingresso $|\psi\rangle = (2, i)^{\mathsf{T}}/\sqrt{5}$ e applichiamo Z. La matrice conserva la prima ampiezza e cambia il segno della seconda. Calcoliamo anche le probabilità per stabilire se la misura computazionale rilevi questa modifica.



La componente b cambia fase; i moduli restano uguali.

$$Z|\psi\rangle = \frac{1}{\sqrt{5}}\begin{pmatrix} 1\cdot 2 + 0\cdot i \\ 0\cdot 2 + (-1)i \end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ -i \end{pmatrix}.$$

$$p_0' = \frac{2^2}{5} = \frac{4}{5}, \qquad p_1' = \frac{(-i)^*(-i)}{5} = \frac{i(-i)}{5} = \frac{-i^2}{5} = \frac{1}{5}.$$

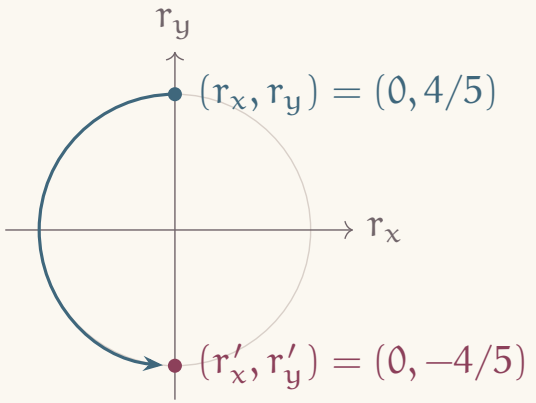
Il segno relativo cambia; le probabilità nella base computazionale restano 4/5 e 1/5. La loro somma è uno.

I moduli quadri restano invariati. La differenza riguarda la fase relativa e diventa visibile nella posizione geometrica dello stato, che calcoliamo di seguito.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $i^2 = -1$, $i^* = -i$; * indica il coniugato.

La geometria del cambio di segno Z

La porta Z dà $a' = a$, $b' = -b$ e conserva i pesi della misura. Ricaviamo le nuove coordinate e applichiamo la mappa a $(2, i)^T/\sqrt{5}$, così da individuare la modifica dello stato.



sezione $r_z = 3/5$

$$
\begin{aligned}
a'^* b' &= a^*(-b) = -a^* b, \\
r'_x &= 2\,\mathrm{Re}(-a^* b) = -2\,\mathrm{Re}(a^* b) = -r_x, \\
r'_y &= 2\,\mathrm{Im}(-a^* b) = -2\,\mathrm{Im}(a^* b) = -r_y, \\
|-b|^2 &= (-b)^*(-b) = (-b^*)(-b) = |b|^2, \\
r'_z &= |a|^2 - |-b|^2 = |a|^2 - |b|^2 = r_z.
\end{aligned}
$$

Sezione $r_z = 3/5$; raggio $4/5$.
Per $r = (0, 4/5, 3/5)$ otteniamo $r' = (0, -4/5, 3/5)$.

Il punto cambia posizione lungo la sezione a quota costante 3/5. Il grafico distingue così stati che la sola distribuzione computazionale lascia indistinti.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^* b)$, $r_y = 2\,\mathrm{Im}(a^* b)$, $r_z = |a|^2 - |b|^2$; Re, Im indicano parte reale e immaginaria. $Z(a,b)^T = (a,-b)^T$. $r = (0, 4/5, 3/5)$; raggio della sezione: $\sqrt{1-(3/5)^2} = \sqrt{16/25} = 4/5$.

Hadamard sui vettori di base

Dopo scambio e cambio di segno, studiamo la ricombinazione: H forma somma e differenza delle ampiezze. Partiamo dai vettori di base $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$, che individuano le colonne della matrice e producono $|+\rangle$ e $|-\rangle$.

prima colonna di H

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

seconda colonna di H

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

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 + 1\cdot 0 \\ 1\cdot 1 - 1\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle.$$

$$H|1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 0 + 1\cdot 1 \\ 1\cdot 0 - 1\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle.$$

$$\||\pm\rangle\|^2 = (1+1)/2 = 1, \qquad \langle + \mid - \rangle = \frac{1\cdot 1 + 1\cdot(-1)}{2} = 0.$$

I due ingressi generano sovrapposizioni ortogonali con uguali probabilità computazionali. La distinzione è nel segno relativo; una seconda Hadamard permetterà di leggerla.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^{\mathsf{T}}/\sqrt{2}$. $\langle v| = (v_0^*, v_1^*)$; $\langle v \mid w\rangle = v_0^* w_0 + v_1^* w_1$, $\|v\|^2 = \langle v \mid v\rangle$. Ortogonalità: $\langle v \mid w\rangle = 0$.

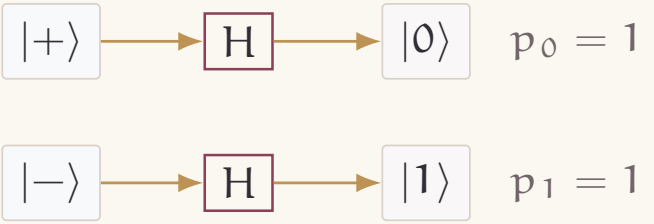
Riconoscere gli stati $|+\rangle$ e $|-\rangle$

Gli stati $|\pm\rangle = (1, \pm 1)^{\mathsf{T}}/\sqrt{2}$ differiscono per un segno e danno gli stessi pesi nella misura computazionale. Applichiamo H prima della misura per verificare se la somma e la differenza delle componenti producano esiti distinguibili.

$$H|+\rangle = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1\cdot 1 \\ 1\cdot 1 - 1\cdot 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 \\ 0 \end{pmatrix} = |0\rangle.$$

$$H|-\rangle = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1\cdot (-1) \\ 1\cdot 1 - 1\cdot (-1) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 \\ 2 \end{pmatrix} = |1\rangle.$$

Per $H|+\rangle$: $(p_0, p_1) = (|1|^2, |0|^2) = (1, 0)$.
Per $H|-\rangle$: $(p_0, p_1) = (|0|^2, |1|^2) = (0, 1)$.



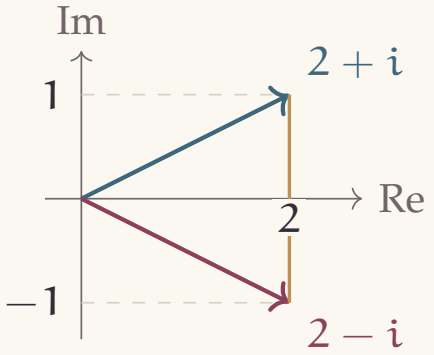
Se l'ingresso appartiene a $\{|+\rangle, |-\rangle\}$, l'esito 0 identifica $|+\rangle$ e l'esito 1 identifica $|-\rangle$.

Le cancellazioni avvengono in componenti diverse: H converte la differenza di segno in due esiti certi distinti. Questa funzione di lettura tornerà nel circuito di Deutsch.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1, \pm 1)^{\mathsf{T}}/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. M_Z indica la misura nella base $(|0\rangle, |1\rangle)$.

Hadamard su due ampiezze complesse

Applichiamo H a $|\psi\rangle = (2, i)^T/\sqrt{5}$. Il piano complesso confronta i numeratori delle ampiezze; i prodotti per il coniugato ne calcolano i moduli quadri.



numeratori delle ampiezze

$$H|\psi\rangle = \frac{1}{\sqrt{10}}\begin{pmatrix} 1\cdot 2 + 1\cdot i \\ 1\cdot 2 - 1\cdot i \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2+i \\ 2-i \end{pmatrix}.$$

$$(2+i)^*(2+i) = (2-i)(2+i) = 4 + 2i - 2i - i^2 = 5.$$

$$(2-i)^*(2-i) = (2+i)(2-i) = 4 - 2i + 2i - i^2 = 5.$$

Entrambe le ampiezze finali hanno modulo $\sqrt{5}/\sqrt{10}$.

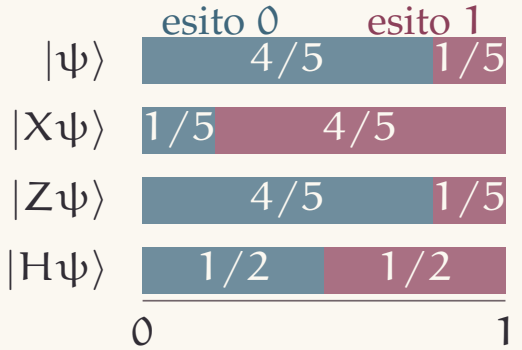
Numeratori di a' (sopra) e b' (sotto); denominatore $\sqrt{10}$.

Le due ampiezze finali sono diverse, mentre i numeratori hanno lo stesso modulo. Dopo aver incluso il fattore di normalizzazione, potremo confrontarne i pesi con quelli di X e Z.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $|z|^2 = z^*z$; ingresso $a = 2/\sqrt{5}$, $b = i/\sqrt{5}$; uscita $a' = (a+b)/\sqrt{2}$, $b' = (a-b)/\sqrt{2}$.

Normalizzazione e probabilità finali

Ripartiamo da $H|\psi\rangle = (2+i, 2-i)^{\mathsf{T}}/\sqrt{10}$. I moduli quadri già sviluppati permettono di verificare la norma e di ricavare la distribuzione. Manteniamo l'ingresso $(2, i)^{\mathsf{T}}/\sqrt{5}$ nel confronto con X e Z.



Ogni barra ha lunghezza totale uno. I colori identificano gli esiti.

$$p_0 = \frac{(2-i)(2+i)}{10} = \frac{5}{10} = \frac{1}{2}, \qquad p_1 = \frac{(2+i)(2-i)}{10} = \frac{5}{10} = \frac{1}{2}.$$

$$\|H|\psi\rangle\|^2 = p_0 + p_1 = \frac{1}{2} + \frac{1}{2} = 1.$$

Sul medesimo ingresso, X dà $(p_0, p_1) = (1/5, 4/5)$, Z dà $(4/5, 1/5)$; H produce $(1/2, 1/2)$.

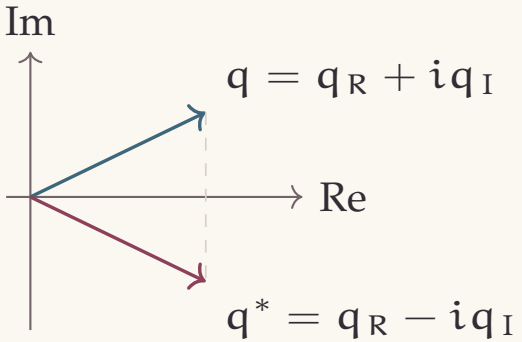
$$\underbrace{(2+i)/\sqrt{10}}_{a'} \longmapsto p_0 = 1/2, \qquad \underbrace{(2-i)/\sqrt{10}}_{b'} \longmapsto p_1 = 1/2.$$

La Hadamard rende uguali i due pesi. Per interpretare questa variazione sulla sfera dobbiamo ricavare come somma e differenza delle ampiezze trasformino le coordinate.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $H(a,b)^{\mathsf{T}} = (a+b, a-b)^{\mathsf{T}}/\sqrt{2}$. $X(a,b)^{\mathsf{T}} = (b,a)^{\mathsf{T}}$. $Z(a,b)^{\mathsf{T}} = (a,-b)^{\mathsf{T}}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $|2 \pm i|^2 = 4 \pm 2i \mp 2i - i^2 = 5$. Gli ingressi del confronto coincidono: $(2, i)^{\mathsf{T}}/\sqrt{5}$.

Le coordinate dopo Hadamard

La porta H trasforma $(a, b)^\mathsf{T}$ in $(a', b')^\mathsf{T} = ((a+b), (a-b))^\mathsf{T}/\sqrt{2}$. Poniamo $q = a^* b = q_\mathrm{R} + i q_\mathrm{I}$, con $q_\mathrm{R} = \operatorname{Re} q$, $q_\mathrm{I} = \operatorname{Im} q$ reali, per ricavare le coordinate orizzontali.



$$q^* - q = -2 i q_\mathrm{I}$$
$$r_x = 2 q_\mathrm{R}, \quad r_y = 2 q_\mathrm{I}$$

$$\begin{aligned} a'^* b' &= (a^* + b^*)(a - b)/2 \\ &= (a^* a - a^* b + b^* a - b^* b)/2 \\ &= (|a|^2 - |b|^2 + b^* a - a^* b)/2, \\ b^* a = q^* &= q_\mathrm{R} - i q_\mathrm{I}, \\ q^* - q &= (q_\mathrm{R} - i q_\mathrm{I}) - (q_\mathrm{R} + i q_\mathrm{I}) = -2 i q_\mathrm{I}, \\ a'^* b' &= (r_z - 2 i q_\mathrm{I})/2 = r_z/2 - i q_\mathrm{I}. \end{aligned}$$

Quindi $r'_x = 2(r_z/2) = r_z$ e $r'_y = 2(-q_\mathrm{I}) = -2 q_\mathrm{I} = -r_y$. La quota r'_z dipende invece dai moduli quadri.

Dalle ampiezze ricaviamo le coordinate orizzontali dell'uscita. Resta da calcolare la quota: essa dipende dalla differenza dei moduli quadri, quindi dalle probabilità.

BASE $|0\rangle = (1,0)^\mathsf{T}$, $|1\rangle = (0,1)^\mathsf{T}$; $(a,b)^\mathsf{T} = a|0\rangle + b|1\rangle$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2 \operatorname{Re}(a^* b)$, $r_y = 2 \operatorname{Im}(a^* b)$, $r_z = |a|^2 - |b|^2$; Re, Im indicano parte reale e immaginaria. $|a|^2 + |b|^2 = 1$; $q_\mathrm{R} = \operatorname{Re} q = r_x/2$, $q_\mathrm{I} = \operatorname{Im} q = r_y/2$. Gli apici indicano l'uscita di H; $q^* = q_\mathrm{R} - i q_\mathrm{I}$.

Hadamard e la quota finale

Le ampiezze dopo Hadamard sono $a' = (a+b)/\sqrt{2}$, $b' = (a-b)/\sqrt{2}$. Per completare la mappa geometrica calcoliamo $|a'|^2 - |b'|^2$: nella sottrazione sopravvivono i termini incrociati che contengono la relazione fra le ampiezze iniziali.

$$\begin{aligned} r_z' &= \frac{(a^*+b^*)(a+b) - (a^*-b^*)(a-b)}{2} \\ &= \frac{|a|^2 + a^*b + b^*a + |b|^2 - |a|^2 + a^*b + b^*a - |b|^2}{2} \\ &= a^*b + b^*a = 2\,\mathrm{Re}(a^*b) = r_x. \end{aligned}$$

$r_x \longrightarrow r_z' = r_x$ $\qquad$ $r_y \longrightarrow r_y' = -r_y$ $\qquad$ $r_z \longrightarrow r_x' = r_z$

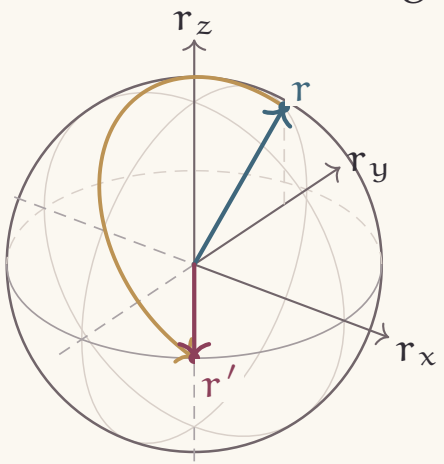
$$H: \quad (r_x, r_y, r_z) \longmapsto (r_z, -r_y, r_x).$$

La nuova quota r_z' coincide con r_x: una relazione fra le ampiezze determina così la differenza dei pesi della misura. Le tre frecce raccolgono la mappa completa, che applicheremo allo stato numerico $(2, i)^T/\sqrt{5}$.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2$; Re, Im indicano parte reale e immaginaria. $H(a,b)^T = (a+b, a-b)^T/\sqrt{2}$. $q = a^*b$, $q^* = b^*a$; $q + q^* = 2\,\mathrm{Re}\,q$. Gli apici indicano l'uscita di H.

Hadamard sullo stato di riferimento

Applichiamo la mappa ottenuta a $|\psi\rangle = (2, i)^T/\sqrt{5}$, con $r = (0, 4/5, 3/5)$. Il calcolo geometrico deve concordare con l'uscita algebrica $H|\psi\rangle = (2+i, 2-i)^T/\sqrt{10}$ e con le sue probabilità uguali.



Ingresso r; uscita r' sull'equatore.
L'arco è un'interpolazione geometrica.

$$r'_x = r_z = 3/5,$$
$$r'_y = -r_y = -4/5,$$
$$r'_z = r_x = 0,$$
$$\|r'\|^2 = 9/25 + 16/25 + 0 = 1.$$

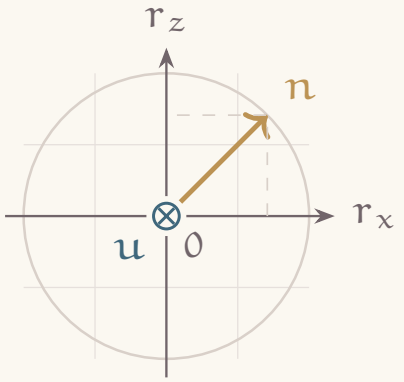
La posizione finale è sull'equatore. Le probabilità già calcolate sono $p_0 = 5/10 = 1/2$ e $p_1 = 5/10 = 1/2$.

L'uscita raggiunge l'equatore, dove la quota nulla corrisponde a pesi uguali. La trasformazione completa ha anche un asse di rotazione, che identifichiamo nella pagina successiva.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $H(a,b)^T = (a+b, a-b)^T/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^*z$. $H : r \mapsto (r_z, -r_y, r_x)$. $|2 \pm i|^2 = 4 \pm 2i \mp 2i - i^2 = 5$; $i^2 = -1$.

L'asse della trasformazione Hadamard

Assumiamo la formula della rotazione di π: per $n \in \mathbb{R}^3$ unitario, $R = 2nn^T - I_3$, dove I_3 è l'identità 3×3. Cerchiamo una direzione fissa della mappa di H: $(x, y, z) \mapsto (z, -y, x)$. Le condizioni $z = x$ e $-y = y$ danno $2y = 0$, quindi $y = 0$. Scegliamo $(1, 0, 1)^T$ e dividiamo per $\sqrt{1^2 + 0^2 + 1^2} = \sqrt{2}$: $n = (1, 0, 1)^T/\sqrt{2}$, $\|n\|^2 = 2/2 = 1$.



$n = (1, 0, 1)^T/\sqrt{2}$

$$2nn^T = \frac{2}{2}\begin{pmatrix}1\\0\\1\end{pmatrix}\begin{pmatrix}1 & 0 & 1\end{pmatrix} = \begin{pmatrix}1\cdot 1 & 1\cdot 0 & 1\cdot 1\\ 0\cdot 1 & 0\cdot 0 & 0\cdot 1\\ 1\cdot 1 & 1\cdot 0 & 1\cdot 1\end{pmatrix} = \begin{pmatrix}1 & 0 & 1\\ 0 & 0 & 0\\ 1 & 0 & 1\end{pmatrix}.$$

$$R = \begin{pmatrix}1-1 & 0-0 & 1-0\\ 0-0 & 0-1 & 0-0\\ 1-0 & 0-0 & 1-1\end{pmatrix} = \begin{pmatrix}0 & 0 & 1\\ 0 & -1 & 0\\ 1 & 0 & 0\end{pmatrix}.$$

$$Rr = (0r_x + 0r_y + 1r_z,\ 0r_x - 1r_y + 0r_z,\ 1r_x + 0r_y + 0r_z)^T = (r_z, -r_y, r_x)^T.$$

La matrice coincide con la mappa di Hadamard: l'asse biseca x e z. Passiamo alla composizione delle porte e alla costruzione delle inverse.

$H(a, b)^T = (a + b, a - b)^T/\sqrt{2}$ agisce sulle ampiezze; R agisce su $r = (r_x, r_y, r_z)^T$. $I_3 = \left(\begin{smallmatrix}1&0&0\\0&1&0\\0&0&1\end{smallmatrix}\right)$. $u = (0, 1, 0)^T$; $n^T u = (1 \cdot 0 + 0 \cdot 1 + 1 \cdot 0)/\sqrt{2} = 0$; $Ru = (u_z, -u_y, u_x)^T = (0, -1, 0)^T = -u$.

Due Hadamard restituiscono l'ingresso

Conosciamo l'effetto delle porte singole. Per studiarne la composizione, cerchiamo prima un'operazione che annulli Hadamard: applicare una seconda H corrisponde al prodotto H^2. Il calcolo della matrice stabilirà il risultato per ogni ingresso.

$$H^2 = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1\cdot 1 & 1\cdot 1 + 1\cdot(-1) \\ 1\cdot 1 + (-1)\cdot 1 & 1\cdot 1 + (-1)(-1) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = I_2.$$

Per $|\chi\rangle = (a, b)^T$, il circuito $|\chi\rangle \xrightarrow{H} H|\chi\rangle \xrightarrow{H} |\chi\rangle$ corrisponde a

$$H^2|\chi\rangle = I_2\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1a + 0b \\ 0a + 1b \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}.$$

Una matrice quadrata U è unitaria se $U^\dagger U = I$. Per H:

$$H^\dagger = (H^*)^T = H^T = H, \qquad H^\dagger H = H^2 = I_2.$$

H^* coniuga gli elementi; $(H^*)^T$ scambia righe e colonne. Poiché H è reale e simmetrica, entrambe le operazioni la conservano.

L'unitarietà conserva la normalizzazione: $\|U\psi\|^2 = (U\psi)^\dagger(U\psi) = \psi^\dagger U^\dagger U\psi = \psi^\dagger I\psi = \|\psi\|^2$. Due Hadamard recuperano l'ingresso; esaminiamo ora le inverse di X e Z.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $U^\dagger = (U^*)^T$; unitaria: $U^\dagger U = UU^\dagger = I$, $U^{-1} = U^\dagger$.

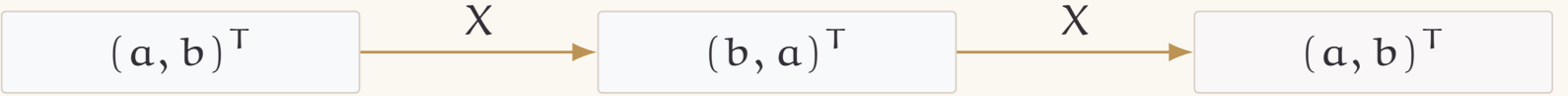
Le inverse di X e Z

La relazione $H^2 = I_2$ ha fornito un circuito che annulla Hadamard. Calcoliamo ogni elemento di X^2 e Z^2 per stabilire se lo scambio delle ampiezze e il cambio di segno possano essere annullati ripetendo la stessa porta.

$$X^2 = \begin{pmatrix} 0\cdot 0 + 1\cdot 1 & 0\cdot 1 + 1\cdot 0 \\ 1\cdot 0 + 0\cdot 1 & 1\cdot 1 + 0\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2,$$

$$Z^2 = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 & 1\cdot 0 + 0(-1) \\ 0\cdot 1 + (-1)0 & 0\cdot 0 + (-1)(-1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2.$$

Dunque $X^{-1} = X$, $Z^{-1} = Z$. Dal calcolo precedente, $H^{-1} = H$.
Anche $X^\dagger = X$ e $Z^\dagger = Z$: le due matrici sono reali e simmetriche. Dunque $X^\dagger X = X^2 = I_2$ e $Z^\dagger Z = Z^2 = I_2$.



Anche X e Z sono le proprie inverse. Per annullare una sequenza servirà inoltre conoscere l'ordine delle operazioni, che confrontiamo usando due circuiti sullo stesso ingresso.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $U^\dagger = (U^*)^T$; unitaria: $U^\dagger U = UU^\dagger = I$, $U^{-1} = U^\dagger$.

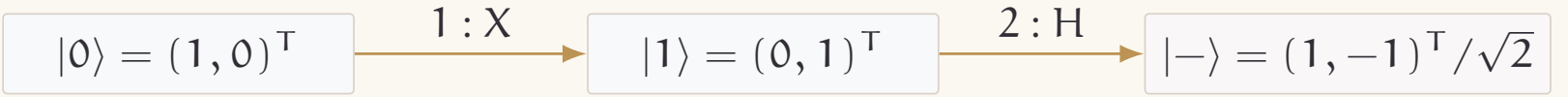
Prima X, poi H

Riprendiamo il circuito iniziale con ingresso $|0\rangle$: prima X, poi H. Costruiamo la matrice complessiva HX, così da collegare la composizione al prodotto delle matrici e confrontarla in seguito con l'ordine opposto.

$$HX = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 0 + 1\cdot 1 & 1\cdot 1 + 1\cdot 0 \\ 1\cdot 0 + (-1)1 & 1\cdot 1 + (-1)0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

$$HX|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 + 1\cdot 0 \\ -1\cdot 1 + 1\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle.$$

$$p_0 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1\cdot 1}{2} = \frac{1}{2}, \qquad p_1 = \left|\frac{-1}{\sqrt{2}}\right|^2 = \frac{(-1)(-1)}{2} = \frac{1}{2}.$$



Il prodotto HX riproduce lo stato meno già ottenuto nella traccia iniziale. Manteniamo ora lo stesso ingresso e scambiamo soltanto l'ordine delle porte.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^T/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$.

Invertire l'ordine delle porte

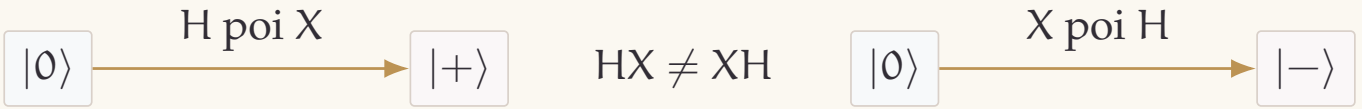
Con lo stesso ingresso $|0\rangle$, applichiamo prima H e poi X. Il confronto fra XH e HX attribuisce all'ordine delle istruzioni la differenza fra le uscite.

$$XH = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot 1 & 0\cdot 1 + 1(-1) \\ 1\cdot 1 + 0\cdot 1 & 1\cdot 1 + 0(-1) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

$$XH|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 - 1\cdot 0 \\ 1\cdot 1 + 1\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle.$$

Le ampiezze finali sono entrambe $1/\sqrt{2}$:

$$p_0 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1\cdot 1}{2} = \frac{1}{2}, \qquad p_1 = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1\cdot 1}{2} = \frac{1}{2}.$$

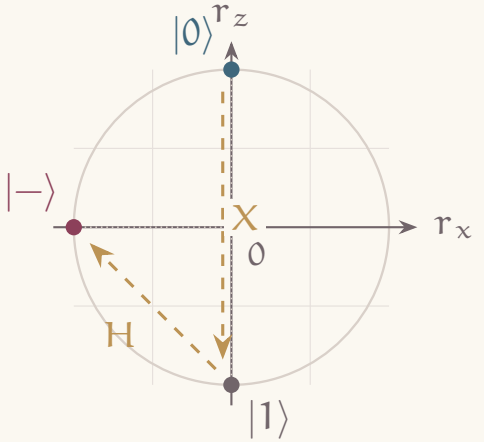


I due circuiti producono stati differenti con la stessa distribuzione computazionale. La geometria consente di seguire le due successioni e individuarne i diversi punti finali.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^T/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $HX = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$; $HX|0\rangle = |-\rangle$.

Prima X, poi H: gli stati sulla sfera

La sequenza X, H su $|0\rangle$ ha dato $HX|0\rangle = |-\rangle$. Ricostruiamo i punti intermedi sulla sfera usando le mappe delle porte: questo confronto verifica che il disegno e il prodotto matriciale descrivano la stessa esecuzione.



Sezione $r_y = 0$

$$
\begin{aligned}
|0\rangle: &\quad r_0 = (0,0,1),\\
X: &\quad r_1 = (0,-0,-1) = (0,0,-1),\\
H: &\quad r_2 = (-1,-0,0) = (-1,0,0).
\end{aligned}
$$

Gli stati intermedi sono $|0\rangle$, $|1\rangle$, $|-\rangle$. Il punto finale è sull'equatore: $p_0 = p_1 = 1/2$.

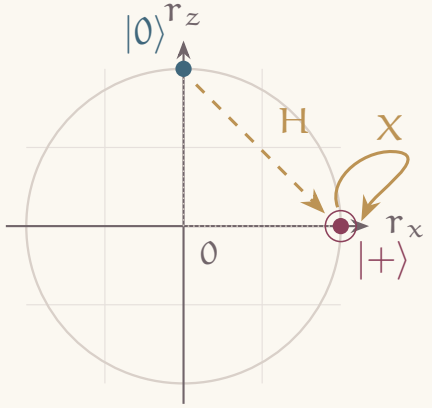
Stati discreti: $r_0 : |0\rangle$, $r_1 : |1\rangle$, $r_2 : |-\rangle$.

Le frecce indicano la successione degli stati dopo ciascuna istruzione. Ripetendo la costruzione nell'ordine opposto potremo confrontare le due esecuzioni sullo stesso spazio geometrico.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $|\pm\rangle = (1,\pm1)^T/\sqrt{2}$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $X : r \mapsto (r_x, -r_y, -r_z)$; $H : r \mapsto (r_z, -r_y, r_x)$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^*z$.

Prima H, poi X: il confronto geometrico

Con ingresso $|0\rangle$, la sequenza H, X dà $XH|0\rangle = |+\rangle$. Seguiamo le coordinate e verifichiamo l'azione di X sullo stato intermedio, per confrontare i due ordini.



$X|+\rangle = |+\rangle$

$r_1 = r_2$: X conserva $|+\rangle$.

$$r_0 = (0,0,1),$$
$$r_1 = (r_{0z}, -r_{0y}, r_{0x}) = (1,0,0),$$
$$r_2 = (r_{1x}, -r_{1y}, -r_{1z}) = (1,0,0).$$

$$X|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle.$$

L'altro ordine dà $HX|0\rangle = |-\rangle = (1,-1)^T/\sqrt{2}$. In entrambi i casi $p_0 = |1/\sqrt{2}|^2 = 1/2$ e $p_1 = |\pm 1/\sqrt{2}|^2 = 1/2$.

X lascia invariato lo stato più preparato da H. L'ordine delle porte determina dunque l'uscita e deve essere considerato anche quando si costruisce il circuito inverso.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^T/\sqrt{2}$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^*b)$, $r_y = 2\,\mathrm{Im}(a^*b)$, $r_z = |a|^2 - |b|^2 = p_0 - p_1$; Re, Im indicano parte reale e immaginaria. $H : r \mapsto (r_z, -r_y, r_x)$; $X : r \mapsto (r_x, -r_y, -r_z)$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^*z$.

L'inversa di una sequenza unitaria

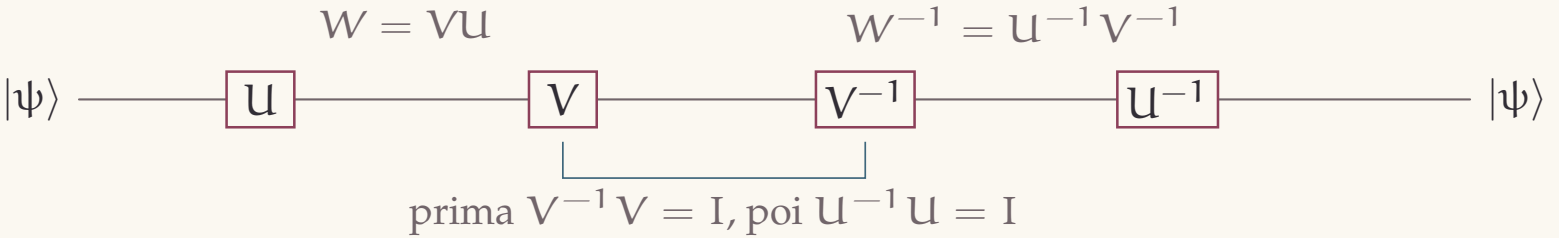
Per invertire una sequenza occorre rispettarne le dipendenze. Se U è seguita da V, l'operatore complessivo è $W = VU$: recuperiamo lo stato precedente annullando prima V, poi U. Verifichiamo algebricamente questa scelta per porte unitarie.

$$(U^{-1}V^{-1})(VU) = U^{-1}(V^{-1}V)U = U^{-1}IU = I.$$

Anche $(VU)(U^{-1}V^{-1}) = V(UU^{-1})V^{-1} = VV^{-1} = I$.

Quindi $W^{-1} = U^{-1}V^{-1}$. Per $W = ZH$ si ha $W^{-1} = HZ$, poiché $H^{-1} = H$ e $Z^{-1} = Z$.

La procedura riguarda la sequenza di porte unitarie prima della misura.



Il circuito inverso percorre le trasformazioni in ordine opposto. Verifichiamo il procedimento su ampiezze complesse, conservando lo stato finale come ingresso dell'inversione.

U, V sono porte unitarie sullo stesso registro; I è l'identità sul registro. $U^\dagger = (U^*)^T$; unitaria: $U^\dagger U = UU^\dagger = I$, $U^{-1} = U^\dagger$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $H^{-1} = H$, $Z^{-1} = Z$. La sequenza considerata precede la misura.

Eseguire H e poi Z

Prepariamo $|\psi\rangle = (2, i)^{\mathsf{T}}/\sqrt{5}$ e applichiamo H, poi Z. La traccia $|\psi\rangle \xrightarrow{\mathrm{H}} \mathrm{H}|\psi\rangle \xrightarrow{\mathrm{Z}} \nu$ individua gli ingressi dei due prodotti; il controllo della norma precede il percorso inverso.

$$\mathrm{H}|\psi\rangle = \frac{1}{\sqrt{10}}\begin{pmatrix} 1\cdot 2 + 1\cdot i \\ 1\cdot 2 - 1\cdot i \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2+i \\ 2-i \end{pmatrix}.$$

$$\mathrm{ZH}|\psi\rangle = \frac{1}{\sqrt{10}}\begin{pmatrix} 1(2+i) + 0(2-i) \\ 0(2+i) - 1(2-i) \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2+i \\ -2+i \end{pmatrix}.$$

$$|2+i|^2 = (2-i)(2+i) = 4 + 2i - 2i - i^2 = 5,$$

$$|-2+i|^2 = (-2-i)(-2+i) = 4 - 2i + 2i - i^2 = 5,$$

$$\|\nu\|^2 = \|\mathrm{ZH}|\psi\rangle\|^2 = (5+5)/10 = 1.$$

Abbiamo ottenuto le due componenti dello stato finale. Ripartiremo da questo vettore per annullare prima Z e poi H, verificando il recupero di entrambe le ampiezze iniziali.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $\mathrm{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $\mathrm{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $\|(a,b)^{\mathsf{T}}\|^2 = |a|^2 + |b|^2$; $|z|^2 = z^* z$. $\nu = \mathrm{ZH}\psi$ è lo stato da invertire; l'inversa di ZH è HZ.

Applicare il circuito inverso

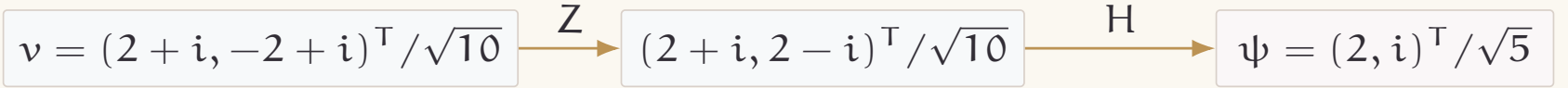
Il circuito diretto ha prodotto $v = (2+i, -2+i)^T/\sqrt{10}$. L'inversa di ZH è HZ: applichiamo prima Z a v, quindi H. Ogni riga mostra come il calcolo recuperi una componente dell'ingresso.

$$Zv = \frac{1}{\sqrt{10}}\begin{pmatrix} 1(2+i) + 0(-2+i) \\ 0(2+i) - 1(-2+i) \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2+i \\ 2-i \end{pmatrix}.$$

$$HZv = \frac{1}{\sqrt{20}}\begin{pmatrix} (2+i) + (2-i) \\ (2+i) - (2-i) \end{pmatrix} = \frac{1}{\sqrt{20}}\begin{pmatrix} 4 \\ 2i \end{pmatrix}.$$

Poiché $\sqrt{20} = 2\sqrt{5}$,

$$HZv = \frac{1}{2\sqrt{5}}\begin{pmatrix} 4 \\ 2i \end{pmatrix} = \frac{1}{\sqrt{5}}\begin{pmatrix} 2 \\ i \end{pmatrix} = |\psi\rangle.$$



Il ritorno a $(2, i)^T/\sqrt{5}$ verifica l'inversione sull'esempio. I prodotti di matrici permettono anche di riconoscere sequenze diverse che realizzano la stessa trasformazione.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. Ingresso da recuperare: $\psi = (2, i)^T/\sqrt{5}$. $H^{-1} = H$, $Z^{-1} = Z$; $(ZH)^{-1} = HZ$; $\sqrt{20} = \sqrt{4 \cdot 5} = 2\sqrt{5}$.

Semplificare H, Z, H

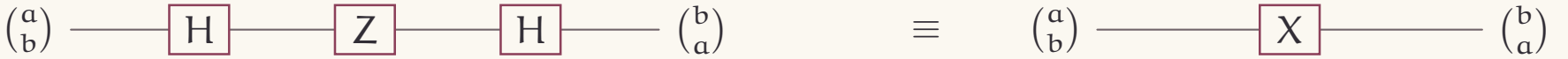
Cerchiamo una descrizione più breve del circuito che applica H, poi Z, poi H. Calcolando HZH e confrontandolo con X, possiamo stabilire l'equivalenza su ogni ingresso e interpretare il ruolo del cambio di segno intermedio.

$$ZH = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 + 0\cdot 1 & 1\cdot 1 + 0(-1) \\ 0\cdot 1 - 1\cdot 1 & 0\cdot 1 + (-1)(-1) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}.$$

Quindi

$$HZH = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1(-1) & 1\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + (-1)(-1) & 1\cdot 1 + (-1)1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix} = X.$$

L'identità $HZH = X$ stabilisce un'equivalenza fra circuiti. Il suo svolgimento mostra anche come un cambio di fase intermedio determini la cancellazione delle ampiezze.

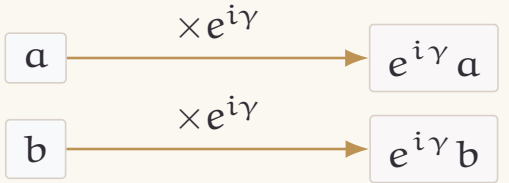


Il circuito a tre porte equivale a X. Per comprendere come il segno introdotto da Z produca questo effetto, distingueremo la fase comune dalla fase relativa fra le ampiezze.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $X(a,b)^T = (b,a)^T$; il prodotto HZH applica le tre porte nell'ordine H, Z, H.

Una fase comune alle ampiezze

Per interpretare $HZH = X$, distinguiamo le modifiche di fase. Confrontiamo $|+\rangle = (1,1)^T/\sqrt{2}$ e $i|+\rangle = (i,i)^T/\sqrt{2}$ nella misura computazionale e dopo H.



lo stesso fattore sulle due componenti

$$|i/\sqrt{2}|^2 = \frac{(-i)i}{2} = \frac{-i^2}{2} = \frac{1}{2}.$$

Nell'esempio $\gamma = \pi/2$ ed $e^{i\gamma} = i$: lo stesso fattore ruota entrambe le ampiezze.

La misura computazionale dà $(1/2, 1/2)$ in entrambi i casi. Dopo H:

$$H(i|+\rangle) = \frac{1}{2}\begin{pmatrix} i+i \\ i-i \end{pmatrix} = \begin{pmatrix} i \\ 0 \end{pmatrix} = i|0\rangle, \quad H|+\rangle = \frac{1}{2}\begin{pmatrix} 1+1 \\ 1-1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

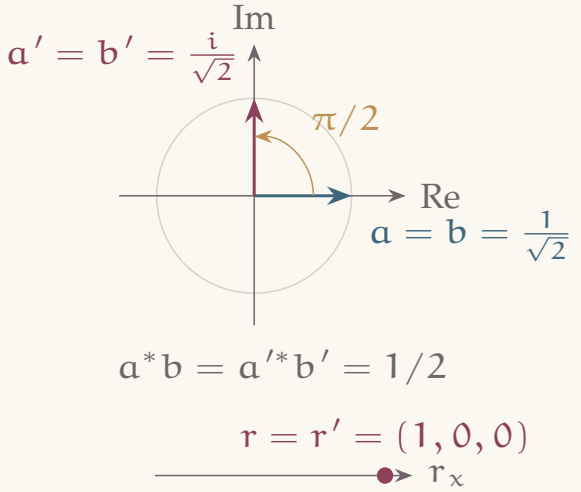
Per $\gamma \in \mathbb{R}$ e un operatore lineare U, si ha $U(e^{i\gamma}|\psi\rangle) = e^{i\gamma}U|\psi\rangle$. Per ogni ampiezza finale c_j, $|e^{i\gamma}c_j|^2 = (e^{i\gamma}c_j)^*(e^{i\gamma}c_j) = e^{-i\gamma}e^{i\gamma}c_j^*c_j = |c_j|^2$.

Un fattore di fase comune resta comune dopo una trasformazione lineare e conserva tutte le probabilità. La rappresentazione geometrica deve quindi assegnare ai due vettori lo stesso punto.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1,\pm1)^T/\sqrt{2}$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $e^{i\gamma} = \cos\gamma + i\sin\gamma$, $\gamma \in \mathbb{R}$; $(e^{i\gamma})^* = e^{-i\gamma}$; $e^{-i\gamma}e^{i\gamma} = 1$. U è lineare: $U(\lambda\psi) = \lambda U\psi$; c_j è la componente j di $U\psi$. $Z(a,b)^T = (a,-b)^T$, $X(a,b)^T = (b,a)^T$.

Una fase comune e la stessa posizione

Per $a' = e^{i\gamma}a$, $b' = e^{i\gamma}b$, con $\gamma \in \mathbb{R}$, verifichiamo l'invarianza geometrica calcolando $a'^* b'$ e i moduli quadri, dai quali dipendono le tre coordinate.



Ampiezze sopra; Bloch sotto.

$$
\begin{aligned}
a'^* b' &= (e^{i\gamma}a)^* (e^{i\gamma}b) \\
&= e^{-i\gamma} e^{i\gamma} a^* b = a^* b, \\
|a'|^2 &= e^{-i\gamma} e^{i\gamma} a^* a = |a|^2, \\
|b'|^2 &= e^{-i\gamma} e^{i\gamma} b^* b = |b|^2.
\end{aligned}
$$

Per $|+\rangle = (1,1)^T/\sqrt{2}$ e $i|+\rangle = (i,i)^T/\sqrt{2}$:

$$a^* b = 1/2, \qquad a'^* b' = (-i)i/2 = -i^2/2 = 1/2.$$

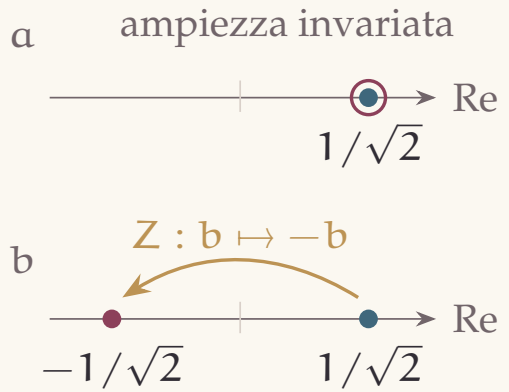
In entrambi i casi $r_x = 2(1/2) = 1$, $r_y = 2 \cdot 0 = 0$, $r_z = 1/2 - 1/2 = 0$: lo stesso punto $r = (1, 0, 0)$.

La fase comune cambia i coefficienti senza spostare il punto sulla sfera. Un cambiamento che riguardi una sola ampiezza può invece modificarne la posizione, come mostra Z.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. Per $|a|^2 + |b|^2 = 1$: $r_x = 2\,\mathrm{Re}(a^* b)$, $r_y = 2\,\mathrm{Im}(a^* b)$, $r_z = |a|^2 - |b|^2$; Re, Im indicano parte reale e immaginaria. $i^2 = -1$, $i^* = -i$; * indica il coniugato. $e^{i\gamma} = \cos\gamma + i\sin\gamma$, $\gamma \in \mathbb{R}$; $(e^{i\gamma})^* = e^{-i\gamma}$; $e^{-i\gamma} e^{i\gamma} = 1$. $Z(a,b)^T = (a,-b)^T$.

Una fase relativa fra due componenti

Partiamo da $|+\rangle = (1,1)^{\mathsf{T}}/\sqrt{2}$ e applichiamo Z: la prima componente resta invariata, la seconda cambia segno. Il confronto con la fase comune permette di individuare l'effetto di una variazione relativa fra le ampiezze.



Righe: ampiezze di $|0\rangle$ e $|1\rangle$. Blu: ingresso; porpora: uscita.

$$Z|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 + 0\cdot 1 \\ 0\cdot 1 - 1\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle.$$

Un fattore comune g dovrebbe soddisfare contemporaneamente $g \cdot 1 = 1$ e $g \cdot 1 = -1$, cioè $g = 1$ e $g = -1$: impossibile.
Nella base computazionale entrambi gli stati danno $(1/2, 1/2)$. La fase relativa richiede una diversa lettura per essere distinta.

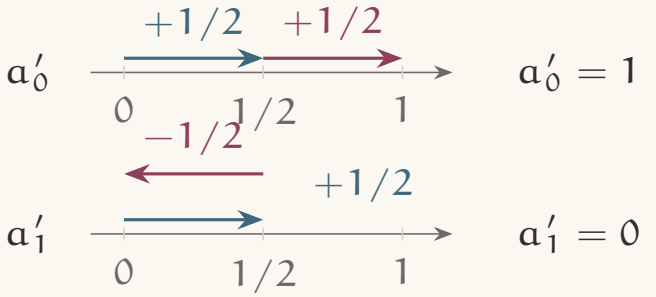
Z trasforma lo stato più nello stato meno, conservando i moduli delle ampiezze. Una Hadamard successiva consentirà di distinguere i due stati mediante le loro cancellazioni.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^{\mathsf{T}}/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. g è l'ipotetico fattore comune alle due ampiezze; a accompagna $|0\rangle$, b accompagna $|1\rangle$.

Ricombinare senza cambio di fase

Prepariamo $|0\rangle$, applichiamo due Hadamard e misuriamo. La prima H crea due ampiezze uguali; la seconda ne forma somma e differenza, che seguiamo separatamente per ciascun esito.





Contributi reali alla seconda Hadamard. Ogni freccia rappresenta un termine della somma che forma un'ampiezza.

a'_j: ampiezza dell'esito j. Ogni contributo vale $(\pm 1/\sqrt{2})(1/\sqrt{2}) = \pm 1/2$.

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1 + 1\cdot 0\\ 1\cdot 1 - 1\cdot 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} \xrightarrow{H} \frac{1}{2}\begin{pmatrix}1+1\\1-1\end{pmatrix} = \begin{pmatrix}1\\0\end{pmatrix}.$$

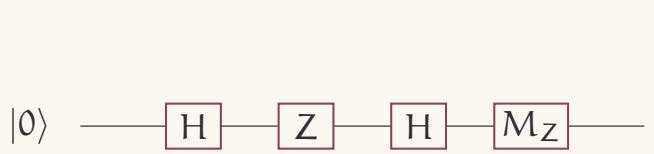
$$p_0 = |1|^2 = 1, \qquad p_1 = |0|^2 = 0.$$

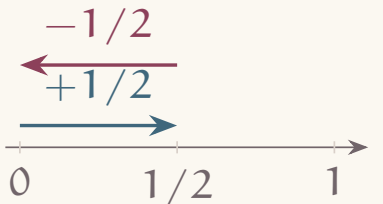
I contributi si sommano per l'esito zero e si cancellano per l'esito uno. Inserendo Z fra le due Hadamard cambierà il segno di uno dei contributi.

BASE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(a,b)^T = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. $|\pm\rangle = (1,\pm 1)^T/\sqrt{2}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $a'_0 = (a+b)/\sqrt{2}$, $a'_1 = (a-b)/\sqrt{2}$; ogni freccia mostra un termine dell'ampiezza. La probabilità si calcola dopo la somma.

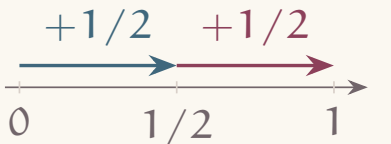
Ricombinare dopo un cambio di segno

Manteniamo $|0\rangle$ e inseriamo Z fra le due Hadamard. Questa sola modifica cambia il segno della seconda ampiezza prima della ricombinazione. Confrontiamo i contributi ai due esiti con quelli del circuito precedente.





a'_0 (esito 0) $= 1/2 - 1/2 = 0$



a'_1 (esito 1) $= 1/2 + 1/2 = 1$

$$H|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1 + 1\cdot 0\\ 1\cdot 1 - 1\cdot 0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad ZH|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1 + 0\cdot 1\\ 0\cdot 1 - 1\cdot 1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}.$$

$$HZH|0\rangle = \frac{1}{2}\begin{pmatrix}1\cdot 1 + 1(-1)\\ 1\cdot 1 - 1(-1)\end{pmatrix} = \frac{1}{2}\begin{pmatrix}0\\2\end{pmatrix} = \begin{pmatrix}0\\1\end{pmatrix}, \quad p_0 = |0|^2 = 0, \quad p_1 = |1|^2 = 1.$$

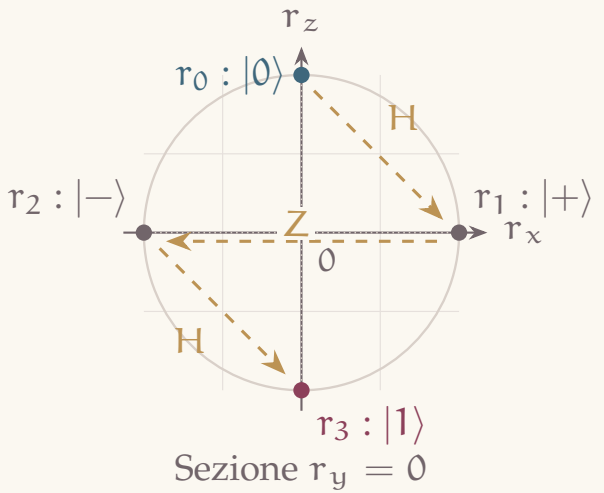
Il cambio di segno trasferisce la cancellazione dalla seconda alla prima componente.

Il cambio di segno sposta la cancellazione sull'esito zero e rende certo l'esito uno. La fase relativa introdotta fra le Hadamard ha quindi modificato il risultato della misura.

DATI E REGOLE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow (a,b)^{\mathsf{T}}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. $Z = \begin{pmatrix}1 & 0\\ 0 & -1\end{pmatrix}$. $p_j = |a_j|^2$: probabilità dell'esito j; $|z|^2 = z^* z$.

La sequenza H, Z, H sulla sfera

I due circuiti hanno mostrato l'effetto di una fase relativa. Seguiamo ora $HZH|0\rangle = |1\rangle$ sulla sfera: la prima Hadamard prepara un punto equatoriale, Z ne cambia la posizione e l'ultima Hadamard determina la quota finale.



Sezione $r_y = 0$

I punti indicano gli stati dopo ogni porta.

$$
\begin{aligned}
r_0 &= (0, 0, 1),\\
r_1 &= (r_{0z}, -r_{0y}, r_{0x}) = (1, 0, 0),\\
r_2 &= (-r_{1x}, -r_{1y}, r_{1z}) = (-1, 0, 0),\\
r_3 &= (r_{2z}, -r_{2y}, r_{2x}) = (0, 0, -1).
\end{aligned}
$$

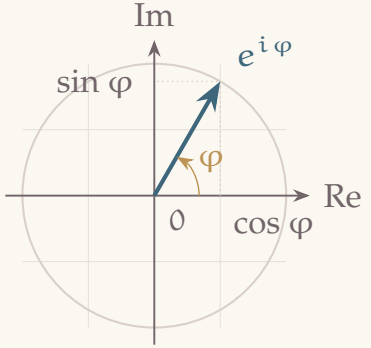
La fase introdotta da Z cambia la componente che si cancella nell'ultima Hadamard.

I numeri identificano gli stati intermedi r_0, r_1, r_2, r_3. Il percorso collega il cambio di segno alla variazione della probabilità; possiamo estendere il confronto a fasi diverse da zero e π.

DATI E REGOLE $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $r = (2\,\mathrm{Re}(a^* b), 2\,\mathrm{Im}(a^* b), |a|^2 - |b|^2)$ per $|\psi\rangle = (a, b)^T$ normalizzato. $H : r \mapsto (r_z, -r_y, r_x)$; $Z : r \mapsto (-r_x, -r_y, r_z)$.

Ricombinare una fase assegnata

Generalizziamo il confronto fra segni opposti introducendo la fase reale φ. Lo stato preparato è $|\psi_\varphi\rangle = (1, e^{i\varphi})^\mathsf{T}/\sqrt{2}$: i moduli restano uguali mentre cambia la relazione fra le ampiezze. Calcoliamo la Hadamard conclusiva.



$|e^{i\varphi}| = 1$

$$\||\psi_\varphi\rangle\|^2 = \frac{1 + e^{-i\varphi}e^{i\varphi}}{2} = \frac{1+1}{2} = 1.$$

$$H|\psi_\varphi\rangle = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1e^{i\varphi} \\ 1\cdot 1 - 1e^{i\varphi}\end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 + e^{i\varphi} \\ 1 - e^{i\varphi}\end{pmatrix}.$$

Le due componenti serviranno al calcolo delle probabilità.

Fattore unitario $e^{i\varphi}$; seconda ampiezza $b = e^{i\varphi}/\sqrt{2}$.

Somma e differenza dipendono dalla fase assegnata. Per trasformare questa dipendenza in probabilità occorre sviluppare i due moduli quadri, includendo i termini incrociati.

DATI E REGOLE $|0\rangle = (1,0)^\mathsf{T}$, $|1\rangle = (0,1)^\mathsf{T}$; $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow (a,b)^\mathsf{T}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1\end{pmatrix}$. $e^{i\varphi} = \cos\varphi + i\sin\varphi$, $(e^{i\varphi})^* = e^{-i\varphi}$, $|e^{i\varphi}| = 1$. $p_j = |a_j|^2$: probabilità dell'esito j; $|z|^2 = z^* z$.

Sviluppare i due moduli quadri

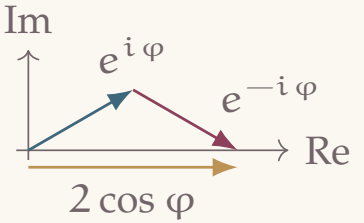
Ripartiamo dalle ampiezze $a_0 = (1 + e^{i\varphi})/2$, $a_1 = (1 - e^{i\varphi})/2$. Il prodotto di ciascuna per il proprio coniugato mostra come la fase relativa entri nelle probabilità. La somma finale ne controlla la normalizzazione.

$$p_0 = \frac{(1 + e^{-i\varphi})(1 + e^{i\varphi})}{4} = \frac{1 + e^{i\varphi} + e^{-i\varphi} + 1}{4} = \frac{2 + 2\cos\varphi}{4} = \frac{1 + \cos\varphi}{2},$$

$$p_1 = \frac{(1 - e^{-i\varphi})(1 - e^{i\varphi})}{4} = \frac{1 - e^{i\varphi} - e^{-i\varphi} + 1}{4} = \frac{2 - 2\cos\varphi}{4} = \frac{1 - \cos\varphi}{2}.$$

$$e^{i\varphi} + e^{-i\varphi} = (\cos\varphi + i\sin\varphi) + (\cos\varphi - i\sin\varphi) = 2\cos\varphi.$$

$$p_0 + p_1 = \frac{1 + \cos\varphi + 1 - \cos\varphi}{2} = \frac{2}{2} = 1.$$



parti immaginarie: $\sin\varphi - \sin\varphi = 0$

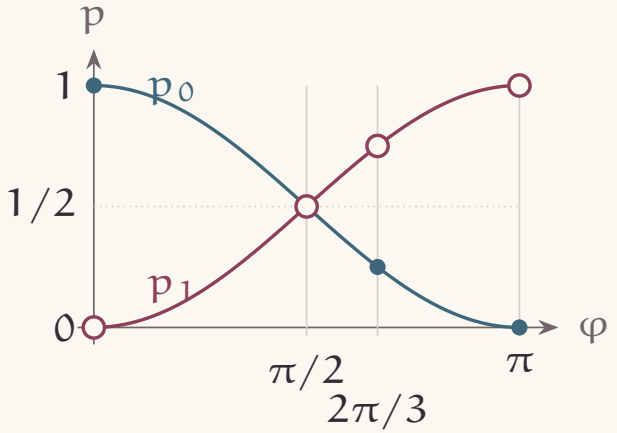
parti reali: $\cos\varphi + \cos\varphi = 2\cos\varphi$

Le parti immaginarie si cancellano e rimane la dipendenza da $\cos\varphi$. La formula consente di passare dagli esiti certi a distribuzioni intermedie modificando soltanto la fase.

DATI E REGOLE $a_0 = (1 + e^{i\varphi})/2$, $a_1 = (1 - e^{i\varphi})/2$: ampiezze dopo H. $p_j = |a_j|^2$: probabilità dell'esito j; $|z|^2 = z^* z$. $e^{i\varphi} = \cos\varphi + i\sin\varphi$, $(e^{i\varphi})^* = e^{-i\varphi}$, $|e^{i\varphi}| = 1$.

Quattro valori della fase

Per l'ingresso $(1, e^{i\varphi})^{\mathsf{T}}/\sqrt{2}$, dopo H vale $p_{0,1} = (1 \pm \cos\varphi)/2$. Confrontiamo quattro valori di φ: sostituire un solo parametro permette di seguire il passaggio fra cancellazione completa e contributi parziali.



p_0: esito 0; p_1: esito 1. Le curve descrivono la misura dopo H; i punti sono i valori della tabella.

φ	$\cos\varphi$	p_0	p_1
0	1	$(1+1)/2 = 1$	$(1-1)/2 = 0$
$\pi/2$	0	$(1+0)/2 = 1/2$	$(1-0)/2 = 1/2$
π	-1	$(1-1)/2 = 0$	$(1+1)/2 = 1$
$2\pi/3$	$-1/2$	$(1-1/2)/2 = 1/4$	$(1+1/2)/2 = 3/4$

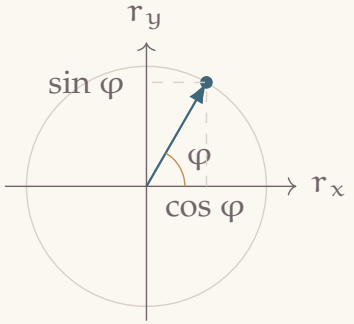
I casi estremi producono un esito certo; gli altri due distribuiscono il peso fra entrambe le uscite.

I punti della tabella appartengono alle curve delle probabilità. Ogni variazione deriva dalla fase relativa dell'ingresso; la rappresentazione geometrica ne mostrerà il significato angolare.

DATI E REGOLE $|\psi_\varphi\rangle = (1, e^{i\varphi})^{\mathsf{T}}/\sqrt{2}$; $H|\psi_\varphi\rangle = \big((1+e^{i\varphi})/2, (1-e^{i\varphi})/2\big)^{\mathsf{T}}$. $p_j = |a_j|^2$: probabilità dell'esito j; $|z|^2 = z^* z$.

La fase relativa percorre l'equatore

Il parametro φ ha determinato le probabilità dopo H. Per interpretarlo geometricamente, ripartiamo da $|\psi_\varphi\rangle = (1, e^{i\varphi})^\top/\sqrt{2}$, con prima ampiezza reale positiva, e calcoliamo le coordinate del punto prima della ricombinazione.



prima di H: $r_z = 0$

dopo H: $r' = (0, -\sin\varphi, \cos\varphi)$
quota $r'_z = \cos\varphi$

Esempio disegnato: $\varphi = \pi/3$.

$$a^* b = \frac{e^{i\varphi}}{2} = \frac{\cos\varphi + i\sin\varphi}{2},$$

$$r_x = 2\frac{\cos\varphi}{2} = \cos\varphi, \quad r_y = 2\frac{\sin\varphi}{2} = \sin\varphi, \quad r_z = \frac{1}{2} - \frac{1}{2} = 0.$$

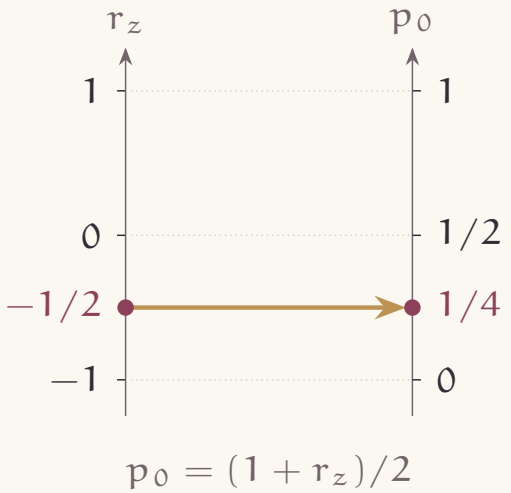
Il fattore $e^{i\varphi}$ ha modulo 1; l'ampiezza $b = e^{i\varphi}/\sqrt{2}$ ha modulo $1/\sqrt{2}$; il vettore r appartiene all'equatore di raggio 1.
La Hadamard dà $r' = (r_z, -r_y, r_x) = (0, -\sin\varphi, \cos\varphi)$: la fase determina la quota finale.

La fase individua una posizione sull'equatore. Hadamard trasferisce questa dipendenza alla quota finale, dalla quale possiamo ricavare direttamente le probabilità di misura.

DATI E REGOLE $a = 1/\sqrt{2}$, $b = e^{i\varphi}/\sqrt{2}$; $r_x = 2\,\mathrm{Re}(a^* b)$, $r_y = 2\,\mathrm{Im}(a^* b)$, $r_z = |a|^2 - |b|^2$; $H : r \mapsto (r_z, -r_y, r_x)$.

La quota geometrica e la regola di Born

Colleghiamo la lettura del grafico alla regola di Born. Per uno stato normalizzato, $r_z = p_0 - p_1$ e $p_0 + p_1 = 1$: queste due relazioni determinano i pesi. Le applichiamo alla quota raggiunta dopo H nel caso $\varphi = 2\pi/3$.



r_z: quota; p_0: probabilità dell'esito 0. Qui $p_0 = 1/4$ e $p_1 = 1 - p_0 = 3/4$.

$$r_z = p_0 - (1 - p_0) = 2p_0 - 1.$$

$$2p_0 = 1 + r_z, \qquad p_0 = \frac{1 + r_z}{2}.$$

$$p_1 = 1 - \frac{1 + r_z}{2} = \frac{2 - 1 - r_z}{2} = \frac{1 - r_z}{2}.$$

Per $r_z' = \cos(2\pi/3) = -1/2$,

$$p_0 = \frac{1 - 1/2}{2} = \frac{1}{4}, \qquad p_1 = \frac{1 + 1/2}{2} = \frac{3}{4}.$$

La corrispondenza fra le due scale è affine: $r_z = -1, 0, 1$ corrisponde a $p_0 = 0, 1/2, 1$.

Il calcolo algebrico e la lettura geometrica forniscono la stessa distribuzione. Per costruire circuiti che conservino insieme un ingresso e un risultato, estendiamo ora la descrizione a due qubit.

DATI E REGOLE $p_j = |a_j|^2$: probabilità dell'esito j; $|z|^2 = z^* z$. $p_0 + p_1 = 1$; $r_z = p_0 - p_1$; dopo H, $r_z' = \cos\varphi$ per $|\psi_\varphi\rangle = (1, e^{i\varphi})^T/\sqrt{2}$.

Le quattro componenti di un registro

Per conservare l'ingresso di una funzione mentre se ne registra il risultato, useremo due qubit. Il registro possiede quattro configurazioni di base. Fissiamo il primo qubit sul filo superiore e l'ordine $\mathcal{B} = (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$.

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Per $|\Psi\rangle = \sum_{x,y=0}^{1} c_{xy}|xy\rangle = c_{00}|00\rangle + c_{01}|01\rangle + c_{10}|10\rangle + c_{11}|11\rangle$ il vettore ha dimensione 4×1 e il simulatore conserva $(c_{00}, c_{01}, c_{10}, c_{11})^{\mathsf{T}}$. L'indice binario è $j = 2^1 x + 2^0 y = 2x + y$: per 10, $j = 2 \cdot 1 + 0 = 2$.

coppia xy	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$
indice j	$j = 0$	$j = 1$	$j = 2$	$j = 3$
ampiezza	c_{00}	c_{01}	c_{10}	c_{11}

Il vettore assegna un'ampiezza a ciascuna coppia. Costruiamolo ora mediante il prodotto tensoriale dei due stati assegnati separatamente.

Base: $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$. In xy, il primo bit pesa 2 e il secondo 1. $j = 2x + y$ parte da zero; la posizione nel vettore è $j + 1$: indice 2, terza componente.

Costruire due stati prodotto

Costruiamo il registro a partire da $|0\rangle = (1,0)^{\mathsf{T}}$ e $|1\rangle = (0,1)^{\mathsf{T}}$. Il prodotto tensoriale associa tutte le coppie di componenti: confrontare $|0\rangle \otimes |1\rangle$ con $|1\rangle \otimes |0\rangle$ chiarisce perché l'ordine dei fattori debba seguire quello dei fili.

$(a,b)^{\mathsf{T}} \otimes (c,d)^{\mathsf{T}}$

	$y=0$	$y=1$
$x=0$	ac	ad
$x=1$	bc	bd

Righe: primo vettore; colonne: secondo. Ordine $00, 01, 10, 11$.

$$\begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix}.$$

$$|0\rangle \otimes |1\rangle = \begin{pmatrix} 1\cdot 0 \\ 1\cdot 1 \\ 0\cdot 0 \\ 0\cdot 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = |01\rangle, \qquad |1\rangle \otimes |0\rangle = \begin{pmatrix} 0\cdot 1 \\ 0\cdot 0 \\ 1\cdot 1 \\ 1\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = |10\rangle.$$

Lo scambio dei fattori cambia la componente occupata. La stessa regola si applica a sovrapposizioni e ampiezze complesse, come nel prossimo esempio.

DATI E REGOLE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow (a,b)^{\mathsf{T}}$. $(a,b)^{\mathsf{T}} \otimes (c,d)^{\mathsf{T}} = (ac, ad, bc, bd)^{\mathsf{T}}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$.

Un prodotto con ampiezze complesse

Scegliamo $u = (3, 4)^{\mathsf{T}}/5$ per assegnare pesi diversi al primo qubit e $v = (1, i)^{\mathsf{T}}/\sqrt{2}$ per introdurre una fase relativa sul secondo, mantenendone uguali i pesi. Il prodotto mostra come queste proprietà si combinino nelle quattro ampiezze. I numeri $3, 4, 5$ rendono immediata la normalizzazione: $\|u\|^2 = (3^2 + 4^2)/25 = (9 + 16)/25 = 1$ e $\|v\|^2 = (1^2 + (-i)i)/2 = (1 - i^2)/2 = 1$. Il prodotto tensoriale costruisce le quattro ampiezze congiunte:

	$\lvert 0\rangle_B$	$\lvert 1\rangle_B$
$\lvert 0\rangle_A$	$c = 3/(5\sqrt{2})$ $p = 9/50$	$c = 3i/(5\sqrt{2})$ $p = 9/50$
$\lvert 1\rangle_A$	$c = 4/(5\sqrt{2})$ $p = 16/50$	$c = 4i/(5\sqrt{2})$ $p = 16/50$

c: ampiezza congiunta; $p = |c|^2$: probabilità. A identifica la riga, B la colonna.

$$u \otimes v = \frac{1}{5\sqrt{2}} \begin{pmatrix} 3 \cdot 1 \\ 3 \cdot i \\ 4 \cdot 1 \\ 4 \cdot i \end{pmatrix} = \frac{1}{5\sqrt{2}} \begin{pmatrix} 3 \\ 3i \\ 4 \\ 4i \end{pmatrix}.$$

L'ordine dei quattro coefficienti segue le righe della griglia: $00, 01, 10, 11$.

I prodotti associano un'ampiezza a ciascuna coppia. Calcoliamo ora i pesi per leggere la griglia in termini di probabilità.

DATI E REGOLE $(a, b)^{\mathsf{T}} \otimes (c, d)^{\mathsf{T}} = (ac, ad, bc, bd)^{\mathsf{T}}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $i^2 = -1$, $i^* = -i$; $|z|^2 = z^* z$.

Leggere i pesi del registro prodotto

Lo stato $u \otimes v = (3, 3i, 4, 4i)^{\mathsf{T}}/(5\sqrt{2})$ proviene da $u = (3, 4)^{\mathsf{T}}/5$ e $v = (1, i)^{\mathsf{T}}/\sqrt{2}$. La griglia permette di confrontare i pesi congiunti e quelli dei singoli qubit.

Nella base $(00, 01, 10, 11)$, la regola di Born dà

$$(p_{00}, p_{01}, p_{10}, p_{11}) = \frac{1}{50}(3^2, (-3i)(3i), 4^2, (-4i)(4i))$$
$$= \frac{1}{50}(9, -9i^2, 16, -16i^2) = \frac{1}{50}(9, 9, 16, 16).$$

	$\lvert 0\rangle_B$	$\lvert 1\rangle_B$
$\lvert 0\rangle_A$	$c = 3/(5\sqrt{2})$ $p = 9/50$	$c = 3i/(5\sqrt{2})$ $p = 9/50$
$\lvert 1\rangle_A$	$c = 4/(5\sqrt{2})$ $p = 16/50$	$c = 4i/(5\sqrt{2})$ $p = 16/50$

La somma è $(9 + 9 + 16 + 16)/50 = 50/50 = 1$.
Le somme per riga restituiscono i pesi del primo qubit:

$$p_A(0) = \frac{9}{50} + \frac{9}{50} = \frac{18}{50} = \frac{9}{25}, \qquad p_A(1) = \frac{16}{50} + \frac{16}{50} = \frac{32}{50} = \frac{16}{25}.$$

Le due colonne hanno lo stesso peso: $p_B(0) = p_B(1) = 9/50 + 16/50 = 25/50 = 1/2$.

Le righe conservano i pesi diversi di u; le colonne hanno i pesi uguali di v. La fase i cambia i coefficienti conservandone i moduli.

DATI E REGOLE $(a, b)^{\mathsf{T}} \otimes (c, d)^{\mathsf{T}} = (ac, ad, bc, bd)^{\mathsf{T}}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $i^2 = -1$, $i^* = -i$; $|z|^2 = z^* z$.

Costruire il prodotto tensoriale di matrici

Per collocare porte locali sul registro, definiamo il prodotto tensoriale: con $A = (a_{jk})$ di dimensione $m \times n$ e B di dimensione $p \times q$, $A \otimes B = (a_{jk}B)_{jk}$ ha dimensione $mp \times nq$.

$$\underbrace{A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}}_{\text{primo fattore}}, \quad \underbrace{B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}}_{\text{secondo fattore}}, \quad A \otimes B = \left(\begin{array}{c|c} aB & bB \\ \hline cB & dB \end{array}\right) = \left(\begin{array}{cc|cc} ae & af & be & bf \\ ag & ah & bg & bh \\ \hline ce & cf & de & df \\ cg & ch & dg & dh \end{array}\right).$$

Per $u = (u_0, u_1)^T$, $v = (v_0, v_1)^T$, la componente (i, j), di indice $2i + j$ con $i, j \in \{0, 1\}$, è

$$\begin{aligned} [(A \otimes B)(u \otimes v)]_{ij} &= A_{i0}B_{j0}u_0v_0 + A_{i0}B_{j1}u_0v_1 \\ &\quad + A_{i1}B_{j0}u_1v_0 + A_{i1}B_{j1}u_1v_1 \\ &= (A_{i0}u_0 + A_{i1}u_1)(B_{j0}v_0 + B_{j1}v_1) = (Au)_i(Bv)_j. \end{aligned}$$

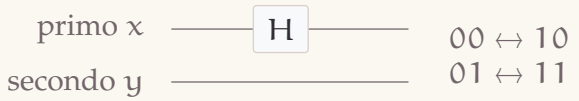
Vale quindi $(A \otimes B)(u \otimes v) = (Au) \otimes (Bv)$. Il primo fattore agisce sul primo qubit, il secondo sul secondo qubit.

La derivazione giustifica il calcolo separato sui fattori di uno stato prodotto. La matrice a blocchi rimane definita sul registro completo e permette di collocare una porta sul filo scelto.

DATI E REGOLE $(a, b)^T \otimes (c, d)^T = (ac, ad, bc, bd)^T$. $A \otimes B = (A_{jk}B)_{jk}$: ogni elemento di A moltiplica l'intera matrice B. i: primo indice; j: secondo indice.

Hadamard sul primo qubit

Usiamo il prodotto tensoriale per collocare H sul primo qubit. L'ingresso è $|00\rangle = (1,0,0,0)^{\mathsf{T}}$; il secondo qubit deve rimanere invariato. Per questo la matrice congiunta è $H \otimes I_2$.



Si combinano coppie con secondo indice fisso.

$$H \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} I_2 & I_2 \\ I_2 & -I_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

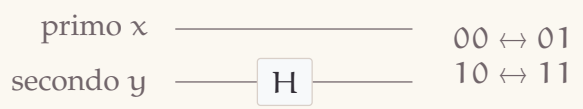
$$(H \otimes I_2)|00\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\cdot 1 + 0\cdot 0 + 1\cdot 0 + 0\cdot 0 \\ 0\cdot 1 + 1\cdot 0 + 0\cdot 0 + 1\cdot 0 \\ 1\cdot 1 + 0\cdot 0 - 1\cdot 0 + 0\cdot 0 \\ 0\cdot 1 + 1\cdot 0 + 0\cdot 0 - 1\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

La Hadamard combina componenti che differiscono nel primo indice. L'identità nel secondo fattore conserva il secondo qubit; spostando la porta cambieranno le coppie coinvolte.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $A \otimes B = (A_{jk}B)_{jk}$.

Hadamard sul secondo qubit

Collochiamo H sul secondo filo e scegliamo $|01\rangle = (0,1,0,0)^{\mathsf{T}}$: il qubit trasformato parte da uno, così vedremo anche il segno negativo di $H|1\rangle$. Rispetto all'esempio precedente cambiano quindi sia il filo sia l'ingresso. Il primo fattore è l'identità e l'operatore diventa $I_2 \otimes H$. I blocchi permettono di individuare le componenti combinate dalla porta.



Si combinano coppie con primo indice fisso.

$$I_2 \otimes H = \begin{pmatrix} H & 0 \\ 0 & H \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

$$(I_2 \otimes H)|01\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1\cdot 0 + 1\cdot 1 + 0\cdot 0 + 0\cdot 0 \\ 1\cdot 0 - 1\cdot 1 + 0\cdot 0 + 0\cdot 0 \\ 0\cdot 0 + 0\cdot 1 + 1\cdot 0 + 1\cdot 0 \\ 0\cdot 0 + 0\cdot 1 + 1\cdot 0 - 1\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \\ 0 \\ 0 \end{pmatrix} = \frac{|00\rangle - |01\rangle}{\sqrt{2}}.$$

La posizione di H stabilisce quali componenti si combinano; il valore iniziale uno determina la differenza dei segni. Il prossimo confronto manterrà fisso l'ingresso e varierà soltanto il filo.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $A \otimes B = (A_{jk}B)_{jk}$.

Scegliere il qubit sul quale agisce X

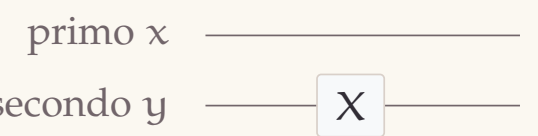
Confrontiamo la posizione di X a parità di ingresso: $|01\rangle = |0\rangle \otimes |1\rangle = (0,1,0,0)^{\mathsf{T}}$, nella base $(00,01,10,11)$. Ogni circuito modifica soltanto il qubit indicato, mentre l'identità conserva l'altro.



$|01\rangle \mapsto |11\rangle$
cambia il primo bit

$$X \otimes I_2 = \begin{pmatrix} 0I_2 & 1I_2 \\ 1I_2 & 0I_2 \end{pmatrix} = \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 1&0&0&0 \\ 0&1&0&0 \end{pmatrix}.$$

$$(X \otimes I_2)|01\rangle = \begin{pmatrix} 0\cdot 0+0\cdot 1+1\cdot 0+0\cdot 0 \\ 0\cdot 0+0\cdot 1+0\cdot 0+1\cdot 0 \\ 1\cdot 0+0\cdot 1+0\cdot 0+0\cdot 0 \\ 0\cdot 0+1\cdot 1+0\cdot 0+0\cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = |11\rangle.$$



$|01\rangle \mapsto |00\rangle$
cambia il secondo bit

$$I_2 \otimes X = \begin{pmatrix} 1X & 0X \\ 0X & 1X \end{pmatrix} = \begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}.$$

$$(I_2 \otimes X)|01\rangle = \begin{pmatrix} 0\cdot 0+1\cdot 1+0\cdot 0+0\cdot 0 \\ 1\cdot 0+0\cdot 1+0\cdot 0+0\cdot 0 \\ 0\cdot 0+0\cdot 1+0\cdot 0+1\cdot 0 \\ 0\cdot 0+0\cdot 1+1\cdot 0+0\cdot 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = |00\rangle.$$

I fili identificano i sottosistemi. Qui lo stato prodotto ammette le etichette separate $|0\rangle$ e $|1\rangle$; per uno stato entangled i due fili resteranno associati a un unico vettore congiunto.

DATI E REGOLE $X = \begin{pmatrix} 0&1 \\ 1&0 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1&0 \\ 0&1 \end{pmatrix}$. Base $(00,01,10,11)$; $A \otimes B = (A_{jk}B)_{jk}$: ciascun elemento A_{jk} moltiplica l'intera matrice B.

Due Hadamard e ingresso 00

Prepariamo $|00\rangle = (1,0,0,0)^{\mathsf{T}}$ e applichiamo una Hadamard su ciascun filo. L'operatore $W = \mathrm{H} \otimes \mathrm{H}$ permette di costruire una sovrapposizione delle quattro configurazioni: seguiamo la formazione di tutte le ampiezze.

ampiezze dopo $\mathrm{H} \otimes \mathrm{H}$

	$y=0$	$y=1$
$x=0$	$1/2$	$1/2$
$x=1$	$1/2$	$1/2$

$$W = \mathrm{H} \otimes \mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} \mathrm{H} & \mathrm{H} \\ \mathrm{H} & -\mathrm{H} \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

$$W|00\rangle = \frac{1}{2} \begin{pmatrix} 1\cdot 1 + 1\cdot 0 + 1\cdot 0 + 1\cdot 0 \\ 1\cdot 1 - 1\cdot 0 + 1\cdot 0 - 1\cdot 0 \\ 1\cdot 1 + 1\cdot 0 - 1\cdot 0 - 1\cdot 0 \\ 1\cdot 1 - 1\cdot 0 - 1\cdot 0 + 1\cdot 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}.$$

Ogni probabilità vale $|1/2|^2 = 1/4$; la somma è $4 \cdot 1/4 = 4/4 = 1$.

Le quattro componenti risultano uguali e positive. Cambiando il secondo bit iniziale manterremo gli stessi moduli, introducendo una configurazione diversa dei segni.

DATI E REGOLE $\mathrm{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $A \otimes B = (A_{jk}B)_{jk}$; $W = \mathrm{H} \otimes \mathrm{H}$.

Due Hadamard e ingresso 01

Manteniamo $W = H \otimes H$ e scegliamo $|01\rangle = (0,1,0,0)^T$. Il confronto con $|00\rangle$ mostra il ruolo della preparazione: il secondo bit modifica i segni delle ampiezze. Questa configurazione sarà utilizzata nel circuito di Deutsch.

$$W|01\rangle = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1\cdot 0 + 1\cdot 1 + 1\cdot 0 + 1\cdot 0 \\ 1\cdot 0 - 1\cdot 1 + 1\cdot 0 - 1\cdot 0 \\ 1\cdot 0 + 1\cdot 1 - 1\cdot 0 - 1\cdot 0 \\ 1\cdot 0 - 1\cdot 1 - 1\cdot 0 + 1\cdot 0 \end{pmatrix}.$$

$$W|01\rangle = \frac{1}{2}\Big(\underbrace{1,-1}_{\text{primo qubit 0}}\ ,\ \underbrace{1,-1}_{\text{primo qubit 1}}\Big)^T = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}.$$

$$W|01\rangle = \frac{|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle \otimes (|0\rangle - |1\rangle)}{2} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} = |+\rangle|-\rangle.$$

Ogni probabilità vale $|\pm 1/2|^2 = 1/4$ e la somma è $4/4 = 1$.

Il risultato si fattorizza in $|+\rangle|-\rangle$. La forma a quattro componenti e la forma prodotto descrivono la stessa preparazione e consentono due modalità equivalenti di calcolo.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $(a,b)^T \otimes (c,d)^T = (ac, ad, bc, bd)^T$.

Due operazioni locali su uno stato prodotto

Riprendiamo $u = (3,4)^{\mathsf{T}}/5$, $v = (1,\mathrm{i})^{\mathsf{T}}/\sqrt{2}$ per verificare il calcolo sui fattori. Con $H \otimes X$, H ricombina u e X scambia v; ricomponiamo le uscite nella base $(00, 01, 10, 11)$.

Primo qubit: $u \xrightarrow{H} Hu$. Secondo qubit: $v \xrightarrow{X} Xv$.

$$Hu = \frac{1}{5\sqrt{2}}\begin{pmatrix} 1\cdot 3 + 1\cdot 4 \\ 1\cdot 3 - 1\cdot 4 \end{pmatrix} = \frac{1}{5\sqrt{2}}\begin{pmatrix} 7 \\ -1 \end{pmatrix}, \qquad Xv = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot \mathrm{i} \\ 1\cdot 1 + 0\cdot \mathrm{i} \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} \mathrm{i} \\ 1 \end{pmatrix}.$$

Il prefattore è $\frac{1}{5\sqrt{2}}\frac{1}{\sqrt{2}} = \frac{1}{5\cdot 2} = \frac{1}{10}$.

prodotti; fattore $1/10$

	$y=0$	$y=1$
$x=0$	$7\mathrm{i}$	7
$x=1$	$-\mathrm{i}$	-1

$$(Hu)\otimes(Xv) = \frac{1}{10}\begin{pmatrix} 7\mathrm{i} \\ 7\cdot 1 \\ (-1)\mathrm{i} \\ (-1)\cdot 1 \end{pmatrix} = \frac{1}{10}\begin{pmatrix} 7\mathrm{i} \\ 7 \\ -\mathrm{i} \\ -1 \end{pmatrix}.$$

La fattorizzazione dell'ingresso rende possibile il calcolo separato. Verifichiamo lo stesso risultato usando la matrice $H \otimes X$ sul vettore congiunto.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $(a,b)^{\mathsf{T}} \otimes (c,d)^{\mathsf{T}} = (ac, ad, bc, bd)^{\mathsf{T}}$. $\mathrm{i}^2 = -1$, $\mathrm{i}^* = -\mathrm{i}$; $|z|^2 = z^* z$. Per un ingresso prodotto, $(A\otimes B)(u\otimes v) = (Au)\otimes(Bv)$.

Verifica mediante la matrice del registro

Ripartiamo da $w = (3, 3i, 4, 4i)^{\mathsf{T}}/(5\sqrt{2})$. Il prodotto per $H \otimes X$ verifica il calcolo sui fattori; i moduli quadri delle quattro componenti forniscono le probabilità congiunte.

$$H \otimes X = \frac{1}{\sqrt{2}} \begin{pmatrix} X & X \\ X & -X \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}.$$

Fattore $1/(\sqrt{2}\,5\sqrt{2}) = 1/10$; numeratore n_{xy}, ampiezza finale $c'_{xy} = n_{xy}/10$.

xy	n_{xy}	$p_{xy} = \lvert n_{xy}\rvert^2/100$
00	$0\cdot 3 + 1(3i) + 0\cdot 4 + 1(4i) = 7i$	$(-7i)(7i)/100 = -49i^2/100 = 49/100$
01	$1\cdot 3 + 0(3i) + 1\cdot 4 + 0(4i) = 7$	$7\cdot 7/100 = 49/100$
10	$0\cdot 3 + 1(3i) + 0\cdot 4 - 1(4i) = -i$	$i(-i)/100 = -i^2/100 = 1/100$
11	$1\cdot 3 + 0(3i) - 1\cdot 4 + 0(4i) = -1$	$(-1)(-1)/100 = 1/100$

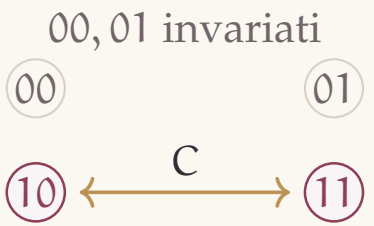
Uscita: $(7i, 7, -i, -1)^{\mathsf{T}}/10$. Norma quadrata: $(49 + 49 + 1 + 1)/100 = 100/100 = 1$.

I due procedimenti coincidono. Abbiamo finora assegnato una porta a ciascun filo; introduciamo ora un'operazione sul bersaglio che dipende dal valore del controllo.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $i^2 = -1$, $i^* = -i$; $|z|^2 = z^* z$.

La CNOT nella base del registro

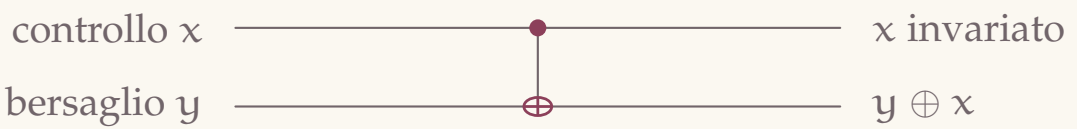
Le porte locali hanno agito separatamente sui due qubit. Introduciamo ora un'operazione il cui effetto sul bersaglio dipende dal valore del controllo, così da produrre correlazioni nello stato congiunto. La CNOT applica X al bersaglio quando il controllo vale uno e lo lascia invariato quando vale zero. Per i bit x, y definiamo $C|x, y\rangle = |x, y \oplus x\rangle$.



Le colonne sono le quattro immagini:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

$\oplus$ indica XOR: $y \oplus 0 = y$ e $y \oplus 1 = 1 - y$.



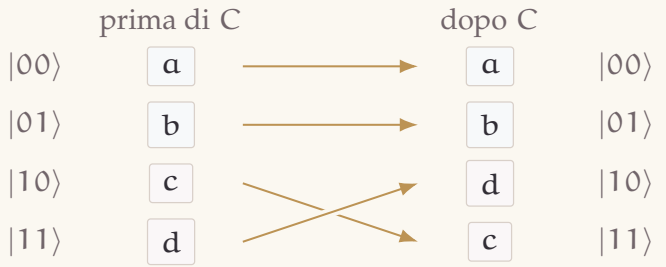
Le immagini dei vettori di base fissano la trasformazione. La matrice la estende per linearità alle sovrapposizioni, mantenendo una descrizione congiunta del registro anche per stati entangled.

DATI E REGOLE Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Controlli di base e vettore generale

Verifichiamo la CNOT sugli ingressi 01 e 11, poi sul vettore generale $v = (a, b, c, d)^{\mathsf{T}}$. Questo passaggio dalla base alla sovrapposizione permette di individuare i contributi conservati e quelli scambiati.

$$C|01\rangle = |0, 1 \oplus 0\rangle = |01\rangle, \qquad C|11\rangle = |1, 1 \oplus 1\rangle = |10\rangle.$$



$$a = c_{00}, b = c_{01}, c = c_{10}, d = c_{11}.$$

Il prodotto sul registro completo dà

$$Cv = \begin{pmatrix} 1a + 0b + 0c + 0d \\ 0a + 1b + 0c + 0d \\ 0a + 0b + 0c + 1d \\ 0a + 0b + 1c + 0d \end{pmatrix} = \begin{pmatrix} a \\ b \\ d \\ c \end{pmatrix}.$$

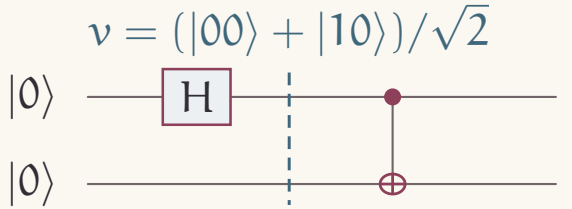
La norma quadrata resta $|a|^2 + |b|^2 + |d|^2 + |c|^2 = \|v\|^2$.

La linearità conserva le ampiezze durante lo scambio. Possiamo quindi preparare una sovrapposizione del controllo e studiare le correlazioni prodotte fra i due qubit.

DATI E REGOLE $C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. a, b, c, d sono coefficienti complessi del vettore congiunto, nell'ordine della base.

Preparare la sovrapposizione iniziale

Per studiare l'effetto della CNOT su una sovrapposizione, partiamo da $|00\rangle$ e applichiamo prima H al controllo. Calcoliamo lo stato intermedio v: esso contiene i due contributi sui quali agirà la porta controllata.



$$v = (H \otimes I_2)|00\rangle = \left[\frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1 + 1\cdot 0\\ 1\cdot 1 - 1\cdot 0\end{pmatrix}\right] \otimes \begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1\\ 1\cdot 0\\ 1\cdot 1\\ 1\cdot 0\end{pmatrix} = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

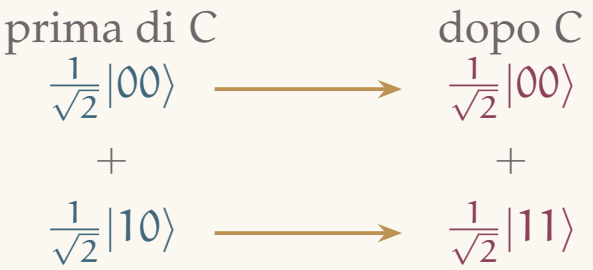
Il bersaglio è ancora nello stato zero, mentre il controllo contiene entrambi i valori di base. Applichiamo la CNOT a ciascun termine conservandone l'ampiezza.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$. $I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow (a,b)^T$. $(a,b)^T \otimes (c,d)^T = (ac, ad, bc, bd)^T$.

Applicare il controllo coerente

La Hadamard ha preparato $v = (|00\rangle + |10\rangle)/\sqrt{2}$. La CNOT lascia fisso il termine con controllo zero e inverte il bersaglio nel termine con controllo uno. L'estensione lineare realizza entrambe le trasformazioni nella stessa sovrapposizione.

$$C|00\rangle = |0, 0 \oplus 0\rangle = |00\rangle, \qquad C|10\rangle = |1, 0 \oplus 1\rangle = |11\rangle.$$



Un unico vettore: due termini di ampiezza $1/\sqrt{2}$. Il termine 10 diventa 11.

Per linearità,

$$Cv = \frac{C|00\rangle + C|10\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = |\Phi^+\rangle.$$

Il vettore è $(1, 0, 0, 1)^T/\sqrt{2}$ e la sua norma quadrata è $(1 + 0 + 0 + 1)/2 = 2/2 = 1$. Lo stato ottenuto è una coppia di Bell.

L'uscita è la coppia di Bell $|\Phi^+\rangle$. I suoi termini hanno indici uguali: la regola di Born permetterà di precisare le correlazioni e le probabilità dei singoli qubit.

DATI E REGOLE $C(a, b, c, d)^T = (a, b, d, c)^T$ nella base $(00, 01, 10, 11)$; $C|xy\rangle = |x, y \oplus x\rangle$. $v = (1, 0, 1, 0)^T/\sqrt{2}$; $|\Phi^+\rangle = (1, 0, 0, 1)^T/\sqrt{2}$.

Probabilità congiunte e marginali

Per $|\Phi^+\rangle = (1,0,0,1)^{\mathsf{T}}/\sqrt{2}$, nella base $(00,01,10,11)$, distinguiamo due letture: le coppie di esiti e i risultati di ciascun qubit, indicati con A e B. Le probabilità marginali si ottengono sommando sulle possibilità dell'altro indice.

	$B=0$	$B=1$	p_A
$A=0$	1/2	0	$p_A(0)=1/2$
$A=1$	0	1/2	$p_A(1)=1/2$
	$p_B(0)$	$p_B(1)$	
	1/2	1/2	

Le somme per riga forniscono p_A; quelle per colonna forniscono p_B.

$$p_{00} = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}, \quad p_{01} = |0|^2 = 0,$$

$$p_{10} = |0|^2 = 0, \qquad p_{11} = \left|\frac{1}{\sqrt{2}}\right|^2 = \frac{1}{2}.$$

$$p_A(0) = p_{00} + p_{01} = \frac{1}{2} + 0 = \frac{1}{2}, \quad p_A(1) = p_{10} + p_{11} = 0 + \frac{1}{2} = \frac{1}{2},$$

$$p_B(0) = p_{00} + p_{10} = \frac{1}{2} + 0 = \frac{1}{2}, \quad p_B(1) = p_{01} + p_{11} = 0 + \frac{1}{2} = \frac{1}{2}.$$

Gli esiti dei due qubit sono sempre uguali; ciascun esito locale ha probabilità 1/2.

Ciascun qubit dà zero e uno con uguale probabilità, mentre i due risultati coincidono sempre. Per descrivere una singola misura occorre anche determinare lo stato condizionato all'esito.

DATI E REGOLE Base $(00,01,10,11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. A: primo qubit; B: secondo; $p_A(x) = \sum_y p_{xy}$, $p_B(y) = \sum_x p_{xy}$.

Misurare il primo qubit

Misuriamo il primo qubit di $|\Phi^+\rangle = (1,0,0,1)^{\mathsf{T}}/\sqrt{2}$, nella base $(00,01,10,11)$. Ciascun proiettore seleziona le componenti compatibili con l'esito; la divisione per $\sqrt{p_j}$ restituisce uno stato di norma uno.

primo qubit: esito 0 $\quad P_0 = \mathrm{diag}(1,1,0,0)$

$$v_0 = P_0|\Phi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1\cdot 1 \\ 1\cdot 0 \\ 0\cdot 0 \\ 0\cdot 1 \end{pmatrix} = \frac{|00\rangle}{\sqrt{2}}.$$

$$p_0 = \|v_0\|^2 = \frac{1+0+0+0}{2} = \frac{1}{2}.$$

$$|\psi_0\rangle = \frac{v_0}{\sqrt{p_0}} = \frac{1/\sqrt{2}}{1/\sqrt{2}}|00\rangle = |00\rangle.$$

primo qubit: esito 1 $\quad P_1 = \mathrm{diag}(0,0,1,1)$

$$v_1 = P_1|\Phi^+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 \\ 0\cdot 0 \\ 1\cdot 0 \\ 1\cdot 1 \end{pmatrix} = \frac{|11\rangle}{\sqrt{2}}.$$

$$p_1 = \|v_1\|^2 = \frac{0+0+0+1}{2} = \frac{1}{2}.$$

$$|\psi_1\rangle = \frac{v_1}{\sqrt{p_1}} = \frac{1/\sqrt{2}}{1/\sqrt{2}}|11\rangle = |11\rangle.$$

I due rami sono esiti alternativi della misura. Se il primo qubit dà j, anche il secondo dà j con certezza in questa base; ciascun ramo iniziale ha probabilità 1/2. Per stabilire l'entanglement dello stato prima della misura esamineremo la fattorizzazione delle sue ampiezze.

DATI E REGOLE Base $(00,01,10,11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. Assumiamo la regola di misura: $v_j = P_j|\psi\rangle$, $p_j = \|v_j\|^2$; se $p_j > 0$, $|\psi_j\rangle = v_j/\sqrt{p_j}$. diag elenca gli elementi diagonali; gli altri sono zero. P_0 conserva le posizioni $00, 01$; P_1 conserva $10, 11$, selezionando il primo indice.

Verificare che lo stato non si fattorizza

La correlazione osservata richiede un esame dello stato. Cerchiamo due vettori il cui prodotto sia $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$: confrontare le quattro ampiezze conduce alle condizioni che una fattorizzazione dovrebbe soddisfare.

$$(a_0|0\rangle + a_1|1\rangle) \otimes (b_0|0\rangle + b_1|1\rangle)$$
$$= a_0b_0|00\rangle + a_0b_1|01\rangle + a_1b_0|10\rangle + a_1b_1|11\rangle.$$

Il confronto con i quattro coefficienti di $|\Phi^+\rangle$ impone

	fattore b_0	fattore b_1
a_0	$a_0b_0 = 1/\sqrt{2}$	$a_0b_1 = 0$
a_1	$a_1b_0 = 0$	$a_1b_1 = 1/\sqrt{2}$

Da $a_0b_0 = 1/\sqrt{2}$ seguono $a_0 \neq 0$, $b_0 \neq 0$; da $a_1b_1 = 1/\sqrt{2}$ seguono $a_1 \neq 0$, $b_1 \neq 0$. Quindi $a_0b_1 \neq 0$, in contraddizione con $a_0b_1 = 0$. La coppia è uno stato entangled.

La fattorizzazione è impossibile. Confrontiamo questa coppia entangled con il prodotto che rappresenterebbe due copie dello stato iniziale.

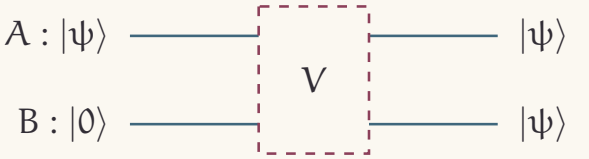
DATI E REGOLE $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $|\psi\rangle = a|0\rangle + b|1\rangle \leftrightarrow (a,b)^T$. $(a,b)^T \otimes (c,d)^T = (ac, ad, bc, bd)^T$. $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$; le quattro ampiezze sono $(1,0,0,1)/\sqrt{2}$.

Clonare uno stato: la trasformazione richiesta

La coppia di Bell ha mostrato che i due registri possono avere esiti correlati. Precisiamo ora la richiesta di clonazione: ricevere uno stato arbitrario in A e produrre due copie indipendenti, descritte dal prodotto dello stesso vettore. Il registro B parte sempre da uno stato fissato $|0\rangle$.

$$V(|\psi\rangle_A \otimes |0\rangle_B) = |\psi\rangle_A \otimes |\psi\rangle_B .$$

Il teorema di non clonazione afferma che nessun unico operatore unitario V può soddisfare questa uguaglianza per ogni stato normalizzato $|\psi\rangle$. La procedura dovrebbe essere la stessa per qualunque ingresso. Uno stato noto può essere preparato più volte. Il teorema riguarda un dispositivo universale che duplichi uno stato arbitrario ricevuto in ingresso.



clonatore universale ipotizzato

Il prodotto in uscita esprime due copie dello stesso stato. Verificheremo il limite usando la linearità.

Cominciamo da due ingressi per i quali la copia è possibile: i vettori della base computazionale.

A: primo qubit; B: ausiliario; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $C = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$; $C|x,y\rangle = |x, y \oplus x\rangle$.

Copiare i vettori della base con la CNOT

Prepariamo il bersaglio B in $|0\rangle$ e usiamo A come controllo. Se A è in uno dei due vettori della base, la regola della CNOT riporta lo stesso valore su entrambi i registri:

$$C(|0\rangle_A|0\rangle_B) = |0, 0 \oplus 0\rangle = |00\rangle = |0\rangle_A|0\rangle_B,$$
$$C(|1\rangle_A|0\rangle_B) = |1, 0 \oplus 1\rangle = |11\rangle = |1\rangle_A|1\rangle_B.$$

La porta riesce quindi a copiare il valore di base anche quando chi la applica ignora se l'ingresso sia zero oppure uno. Per verificare la richiesta universale, occorre includere anche le sovrapposizioni. Scegliamo $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e prepariamo

$$|+\rangle_A|0\rangle_B = \frac{|0\rangle_A|0\rangle_B + |1\rangle_A|0\rangle_B}{\sqrt{2}} = \frac{|00\rangle + |10\rangle}{\sqrt{2}}.$$

Questa espressione consente di usare le due immagini appena calcolate, conservando il coefficiente $1/\sqrt{2}$ in ciascun termine.

La stessa porta agisce ora sulla sovrapposizione. Confrontiamo l'uscita determinata dalla linearità con due copie dello stato $|+\rangle$.

A: primo qubit; B: ausiliario; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $C = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$; $C|x, y\rangle = |x, y \oplus x\rangle$.

Confrontare la coppia di Bell con due copie

Prepariamo A in $|+\rangle$ e B in $|0\rangle$. La linearità determina l'uscita della CNOT a partire dai due casi di base:

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

Per avere due copie, entrambi i fattori dovrebbero invece essere $|+\rangle$. Sviluppiamo il prodotto richiesto:

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

Uscita della CNOT

	$y=0$	$y=1$
$x=0$	$1/\sqrt{2}$	0
$x=1$	0	$1/\sqrt{2}$

Due copie richieste

	$y=0$	$y=1$
$x=0$	$1/2$	$1/2$
$x=1$	$1/2$	$1/2$

Le righe indicano A, le colonne B. Le celle 01 e 10 valgono zero nell'uscita effettiva e 1/2 nel prodotto richiesto: i due stati sono differenti.

La CNOT produce una coppia entangled. Verifichiamo ora che il limite dipende dalla linearità di qualsiasi candidato clonatore.

A: primo qubit; B: ausiliario; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $C = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$; $C|x,y\rangle = |x, y \oplus x\rangle$.

Dimostrare il limite per ogni operatore unitario

Supponiamo che un operatore unitario V cloni ogni stato, usando un secondo registro inizializzato nello stesso stato normalizzato $|b\rangle$. La richiesta applicata ai vettori di base impone

$$V(|0\rangle|b\rangle) = |00\rangle, \qquad V(|1\rangle|b\rangle) = |11\rangle.$$

Ogni operatore unitario è lineare. Applicando la linearità a $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ otteniamo pertanto

$$\begin{aligned} V(|+\rangle|b\rangle) &= V\left(\frac{|0\rangle|b\rangle + |1\rangle|b\rangle}{\sqrt{2}}\right) \\ &= \frac{V(|0\rangle|b\rangle) + V(|1\rangle|b\rangle)}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \end{aligned}$$

La richiesta di clonazione darebbe invece $|+\rangle|+\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)/2$. Il coefficiente di $|01\rangle$ dovrebbe essere contemporaneamente 0 e 1/2: la contraddizione esclude un tale V. La dimostrazione vale per qualsiasi stato iniziale fissato $|b\rangle$ dell'ausiliario.

I fili continuano a identificare i sistemi fisici anche quando lo stato è entangled. Riprendiamo la coppia di Bell e calcoliamo una porta locale.

A: primo qubit; B: ausiliario; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $V(\alpha u + \beta v) = \alpha Vu + \beta Vv$; $\alpha, \beta \in \mathbb{C}$. $|b\rangle$: stato fissato del secondo registro, distinto dal nome B.

Una porta locale su una coppia entangled

Per trasformare esiti uguali in esiti opposti, applichiamo X al primo qubit di $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$. Seguiamo per linearità lo scambio del primo indice nei due termini dello stato congiunto.

prima

	$y=0$	$y=1$
$x=0$	$1/\sqrt{2}$	0
$x=1$	0	$1/\sqrt{2}$

dopo

	$y=0$	$y=1$
$x=0$	0	$1/\sqrt{2}$
$x=1$	$1/\sqrt{2}$	0

$$X|0\rangle = \begin{pmatrix} 0\cdot 1 + 1\cdot 0 \\ 1\cdot 1 + 0\cdot 0 \end{pmatrix} = |1\rangle, \quad X|1\rangle = \begin{pmatrix} 0\cdot 0 + 1\cdot 1 \\ 1\cdot 0 + 0\cdot 1 \end{pmatrix} = |0\rangle.$$

$$(X \otimes I_2)|\Phi^+\rangle = \frac{(X|0\rangle)\otimes|0\rangle + (X|1\rangle)\otimes|1\rangle}{\sqrt{2}} = \frac{|1\rangle\otimes|0\rangle + |0\rangle\otimes|1\rangle}{\sqrt{2}} = \frac{|10\rangle + |01\rangle}{\sqrt{2}}.$$

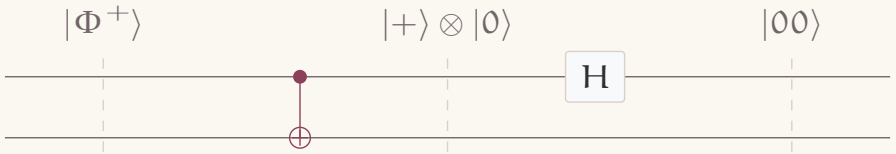
All'ingresso: $p_{00} = p_{11} = |1/\sqrt{2}|^2 = 1/2$, $p_{01} = p_{10} = |0|^2 = 0$. All'uscita: $p_{01} = p_{10} = 1/2$, $p_{00} = p_{11} = 0$. Gli esiti passano da uguali a opposti. Ciascuna griglia descrive entrambi i qubit.

X cambia le correlazioni da esiti uguali a esiti opposti. Le probabilità iniziali si ottengono anche preparando 00 oppure 11, ciascuno con probabilità 1/2: la prova dell'entanglement riguarda le ampiezze dello stato puro.

DATI E REGOLE $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Base $(00, 01, 10, 11)$; c_{xy} è l'ampiezza di $|xy\rangle$; $p_{xy} = |c_{xy}|^2$. $(A \otimes B)(u \otimes v) = (Au) \otimes (Bv)$, applicata a ogni termine per linearità.

Invertire la preparazione di Bell

Completiamo lo studio della preparazione di Bell invertendone il circuito. Ripartiamo da $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$, prima di una misura: annulliamo la CNOT, poi applichiamo H al primo qubit per recuperare $|00\rangle$.



$$C|\Phi^+\rangle = \frac{C|00\rangle + C|11\rangle}{\sqrt{2}} = \frac{|00\rangle + |10\rangle}{\sqrt{2}} = |+\rangle|0\rangle.$$

$$(H \otimes I_2)|+\rangle|0\rangle = \left[\frac{1}{2}\begin{pmatrix}1+1\\1-1\end{pmatrix}\right] \otimes \begin{pmatrix}1\\0\end{pmatrix} = |0\rangle|0\rangle = |00\rangle.$$

$$(a,b,c,d)^T \xrightarrow{C} (a,b,d,c)^T \xrightarrow{C} (a,b,c,d)^T.$$

Quindi $C^2 = I_4$, con $I_4 = \mathrm{diag}(1,1,1,1)$; inoltre $H^2 = I_2$.

La CNOT ha mostrato come un controllo condizioni lo scambio del bersaglio. Introduciamo ora due controlli per registrare il valore di AND in un terzo qubit.

DATI E REGOLE $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$. $I_2 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$. $|\pm\rangle = (1,\pm1)^T/\sqrt{2}$. $C|xy\rangle = |x, y \oplus x\rangle$; $00 \mapsto 00$, $01 \mapsto 01$, $10 \mapsto 11$, $11 \mapsto 10$. $|\Phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$; $H^2 = I_2$.

Calcolare AND conservando i due ingressi

L'AND di due bit vale uno soltanto quando entrambi valgono uno. Per conservare gli ingressi a, b, registriamo il risultato in un terzo bit t, inizializzato a zero. La porta che realizza questo aggiornamento è la *Toffoli*.

a	b	$a \wedge b = ab$	uscita (a, b, t')
0	0	$0 \cdot 0 = 0$	$(0, 0, 0)$
0	1	$0 \cdot 1 = 0$	$(0, 1, 0)$
1	0	$1 \cdot 0 = 0$	$(1, 0, 0)$
1	1	$1 \cdot 1 = 1$	$(1, 1, 1)$

Le quattro uscite restano distinte: i primi due bit identificano l'ingresso.



$$T|a, b, 0\rangle = |a, b, ab\rangle, \qquad T|1, 1, 0\rangle = |1, 1, 1 \cdot 1\rangle = |1, 1, 1\rangle.$$

Il solo valore AND coincide per $00, 01, 10$. Conservare anche a, b rende possibile recuperare la coppia che ha prodotto quel risultato.

Definiamo l'aggiornamento anche per un ausiliario inizializzato a uno, quindi lo eseguiamo su tutti gli ingressi della base.

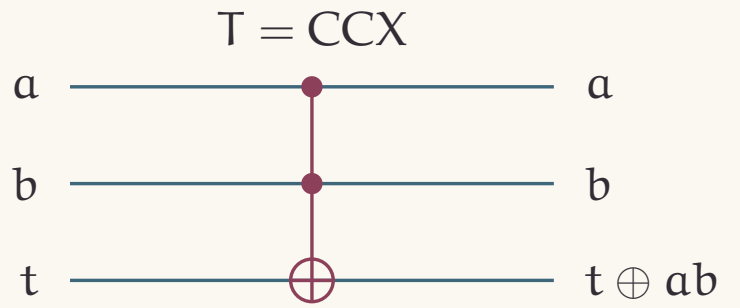
a, b: bit di ingresso; t: bit ausiliario; t': suo valore in uscita. $a \wedge b = ab$: AND. $|a, b, t\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

La regola completa della porta di Toffoli

Toffoli, indicata con T o CCX, conserva i due controlli a, b e aggiorna il bersaglio mediante XOR. Per $ab = 0$ il bersaglio resta uguale; per $ab = 1$ cambia valore:

$$T|a, b, t\rangle = |a, b, t \oplus ab\rangle, \qquad t \oplus 0 = t, \quad t \oplus 1 = 1 - t.$$

abt	$t \oplus ab$	uscita
000	$0 \oplus (0 \cdot 0) = 0$	000
001	$1 \oplus (0 \cdot 0) = 1$	001
010	$0 \oplus (0 \cdot 1) = 0$	010
011	$1 \oplus (0 \cdot 1) = 1$	011
100	$0 \oplus (1 \cdot 0) = 0$	100
101	$1 \oplus (1 \cdot 0) = 1$	101
110	$0 \oplus (1 \cdot 1) = 1$	111
111	$1 \oplus (1 \cdot 1) = 0$	110



I punti individuano i due controlli. Il simbolo $\oplus$ sul terzo filo indica lo scambio $0 \leftrightarrow 1$, attivo quando $a = b = 1$.

Con $t = 0$, il risultato è $t' = 0 \oplus ab = ab$. Con $t = 1$ e $a = b = 1$, il risultato è $t' = 1 \oplus 1 = 0$.

La tabella descrive l'intera porta. I due esempi seguenti svolgono separatamente i calcoli con ausiliario zero e con ausiliario uno.

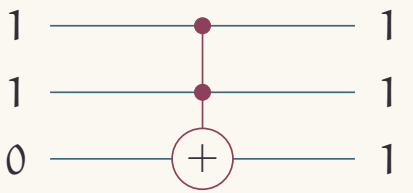
$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; $a, b, t \in \{0, 1\}$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. I tre fili identificano tre qubit; le etichette con bit descrivono l'azione sui vettori della base.

Calcolare AND con memoria iniziale zero

Fissiamo $t = 0$ e consideriamo le quattro coppie dei controlli. Calcoliamo prima ab, poi aggiorniamo il terzo bit mediante XOR; i primi due bit restano disponibili in uscita.

abt	ab	$t \oplus ab$	$T\|abt\rangle$
000	$0 \cdot 0 = 0$	$0 \oplus 0 = 0$	$\|000\rangle$
010	$0 \cdot 1 = 0$	$0 \oplus 0 = 0$	$\|010\rangle$
100	$1 \cdot 0 = 0$	$0 \oplus 0 = 0$	$\|100\rangle$
110	$1 \cdot 1 = 1$	$0 \oplus 1 = 1$	$\|111\rangle$

Con $t = 0$ si ha $t \oplus ab = 0 \oplus ab = ab$: leggere il terzo bit fornisce il valore di AND. L'uscita 111 proviene dalla coppia 11.



Il circuito evidenzia il caso con entrambi i controlli attivi.

Con memoria iniziale zero, il terzo bit restituisce AND. Manteniamo gli stessi controlli e cambiamo la memoria iniziale.

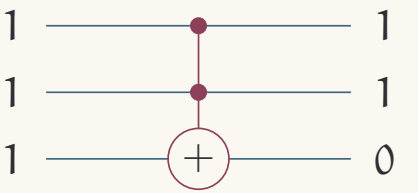
$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$.

Cambiare il valore iniziale della memoria

Fissiamo $t = 1$ e consideriamo le quattro coppie dei controlli. Calcoliamo prima ab, poi aggiorniamo il terzo bit mediante XOR; i primi due bit restano disponibili in uscita.

abt	ab	$t \oplus ab$	$T\lvert abt\rangle$
001	$0 \cdot 0 = 0$	$1 \oplus 0 = 1$	$\lvert 001\rangle$
011	$0 \cdot 1 = 0$	$1 \oplus 0 = 1$	$\lvert 011\rangle$
101	$1 \cdot 0 = 0$	$1 \oplus 0 = 1$	$\lvert 101\rangle$
111	$1 \cdot 1 = 1$	$1 \oplus 1 = 0$	$\lvert 110\rangle$

Con $t = 1$ si ha $t \oplus ab = 1 \oplus ab = 1 - ab$. Per i controlli 11 l'ausiliario torna a zero; per le altre coppie resta uno. La preparazione della memoria determina il significato del bit letto.



Il circuito evidenzia il caso con entrambi i controlli attivi.

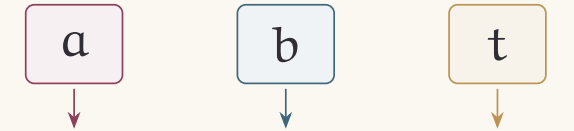
Abbiamo determinato le otto immagini della base. Per disporle nelle colonne della matrice occorre prima associare ogni stringa di tre bit a un indice numerico.

$T\lvert a, b, t\rangle = \lvert a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $\lvert abt\rangle = \lvert a\rangle \otimes \lvert b\rangle \otimes \lvert t\rangle$.

Dalla stringa di bit all'indice del vettore

Per costruire la matrice di Toffoli numeriamo gli otto stati di base da zero a sette. Scegliamo l'ordine binario: in abt, il bit a pesa quattro, b pesa due e t pesa uno. Sommiamo i tre contributi per ottenere j.

stato	calcolo	j
$\lvert 000\rangle$	$4\cdot 0+2\cdot 0+0$	0
$\lvert 001\rangle$	$4\cdot 0+2\cdot 0+1$	1
$\lvert 010\rangle$	$4\cdot 0+2\cdot 1+0$	2
$\lvert 011\rangle$	$4\cdot 0+2\cdot 1+1$	3
$\lvert 100\rangle$	$4\cdot 1+2\cdot 0+0$	4
$\lvert 101\rangle$	$4\cdot 1+2\cdot 0+1$	5
$\lvert 110\rangle$	$4\cdot 1+2\cdot 1+0$	6
$\lvert 111\rangle$	$4\cdot 1+2\cdot 1+1$	7



$$j = 4a + 2b + t$$

Il bit t cambia a ogni incremento; b ogni due e a ogni quattro.

L'indice 6 indica la settima componente: si conta da zero.

Questa convenzione fissa l'ordine delle componenti e delle righe e colonne della matrice. Usiamo ora lo stato 110 per collegare l'indice 6 al prodotto tensoriale e all'azione di Toffoli.

$a, b, t \in \{0, 1\}$; $\lvert abt\rangle = \lvert a\rangle \otimes \lvert b\rangle \otimes \lvert t\rangle$. a: primo controllo; b: secondo controllo; t: bersaglio. $j = 4a + 2b + t \in \{0, \ldots, 7\}$; posizione contata da uno $= j + 1$.

Dalle immagini della base alla matrice di Toffoli

Riprendiamo la base $\mathcal{B}_3 = (000, 001, 010, 011, 100, 101, 110, 111)$ e l'indice binario $j = 4a + 2b + t$. Per 110, $j = 4 \cdot 1 + 2 \cdot 1 + 0 = 6$. Il prodotto tensoriale conferma la posizione del valore 1 nel vettore:

$$|11\rangle = (0,1)^T \otimes (0,1)^T = (0 \cdot 0, 0 \cdot 1, 1 \cdot 0, 1 \cdot 1)^T = (0,0,0,1)^T.$$

$$|110\rangle = |11\rangle \otimes |0\rangle = \begin{pmatrix} 0 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \\ 0 \cdot 0 \\ 0 \cdot 1 \\ 0 \cdot 0 \\ 1 \cdot 1 \\ 1 \cdot 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}.$$

Indice 6: il valore 1 è in settima posizione.

$$T = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

La colonna j contiene $T|abt\rangle$.
$110 \mapsto 111$: colonna 6, riga 7.
$111 \mapsto 110$: colonna 7, riga 6.

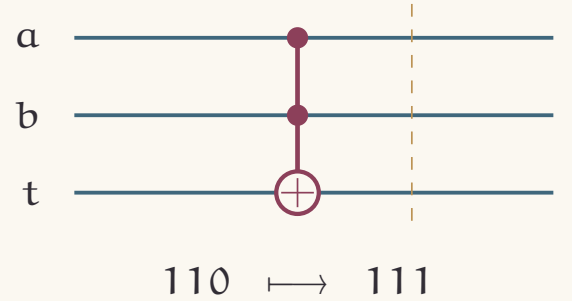
I due controlli di 110 attivano Toffoli. La settima colonna ne contiene l'immagine, che verifichiamo sviluppando gli otto prodotti di riga.

$T|a,b,t\rangle = |a,b,t \oplus ab\rangle$; $a,b,t \in \{0,1\}$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $j = 4a + 2b + t$; indice j, posizione $j+1$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $(u_0,u_1)^T \otimes v = (u_0 v, u_1 v)^T$. Le colonne 0–5 restano invariate.

Moltiplicare la matrice di Toffoli per un ingresso

Usiamo la base $(000, 001, 010, 011, 100, 101, 110, 111)$. L'ingresso è $v = |110\rangle = (0,0,0,0,0,0,1,0)^T$. Ogni componente dell'uscita si ottiene moltiplicando una riga di T per v.

$$T = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$



Il prodotto matriciale deve riprodurre lo scambio indicato dalla porta.

Le prime sei righe conservano le prime sei componenti; le ultime due righe scambiano le posizioni di indice 6 e 7.

Nella pagina successiva esplicitiamo gli otto prodotti di riga usando questa stessa matrice.

$T|a,b,t\rangle = |a,b,t \oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. v_j: componente di indice j; $j = 0, \ldots, 7$.

Eseguire gli otto prodotti di riga

Ripartiamo da $v = (0,0,0,0,0,0,1,0)^T$ e calcoliamo $w = Tv$. Ogni riga comprende tutti gli otto prodotti della matrice precedente.

$$
\begin{aligned}
w_0 &= 1\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_1 &= 0\cdot 0 + 1\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_2 &= 0\cdot 0 + 0\cdot 0 + 1\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_3 &= 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 1\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_4 &= 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 1\cdot 0 + 0\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_5 &= 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 1\cdot 0 + 0\cdot 1 + 0\cdot 0 = 0\\
w_6 &= 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 1 + 1\cdot 0 = 0\\
w_7 &= 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 0\cdot 0 + 1\cdot 1 + 0\cdot 0 = 1
\end{aligned}
$$

Il risultato è $w = (0,0,0,0,0,0,0,1)^T = |111\rangle$. La componente unitaria si trova ora nell'ottava posizione.

L'ampiezza passa da 110 a 111 e la norma resta uno. Applichiamo nuovamente Toffoli per verificare il recupero dell'ingresso.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000,001,010,011,100,101,110,111)$; $|abt\rangle = |a\rangle\otimes|b\rangle\otimes|t\rangle$. $w_i = \sum_{j=0}^{7} T_{ij}v_j$; la matrice completa è riprodotta nella pagina precedente.

Applicare due volte la stessa porta

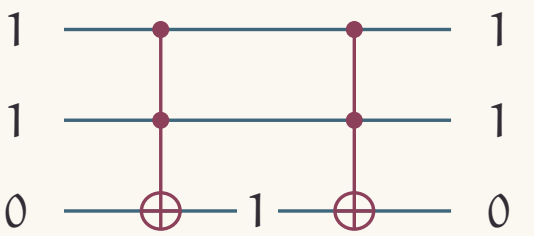
Verifichiamo la reversibilità su due ingressi, mantenendo invariati i controlli fra la prima e la seconda applicazione. Per 110, il prodotto dei controlli è $1 \cdot 1 = 1$:

$$T|110\rangle = |11, 0 \oplus 1\rangle = |111\rangle, \qquad T|111\rangle = |11, 1 \oplus 1\rangle = |110\rangle.$$

Per 100, il prodotto è $1 \cdot 0 = 0$ e le due applicazioni conservano il bersaglio:

$$T|100\rangle = |10, 0 \oplus 0\rangle = |100\rangle,$$

$$T|100\rangle = |10, 0 \oplus 0\rangle = |100\rangle.$$



In entrambi i casi l'uscita finale coincide con l'ingresso. La seconda porta usa nuovamente gli stessi due controlli.

I due calcoli suggeriscono una proprietà valida su tutta la base. La dimostriamo prima di estenderla alle sovrapposizioni.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$.

Invertire Toffoli e verificarne l'unitarietà

Poiché i controlli restano invariati, applicare nuovamente Toffoli usa lo stesso prodotto ab. Seguiamo entrambe le trasformazioni sul medesimo ingresso:

$$T^2|a,b,t\rangle = T|a,b,t\oplus ab\rangle = |a,b,(t\oplus ab)\oplus ab\rangle = |a,b,t\rangle.$$

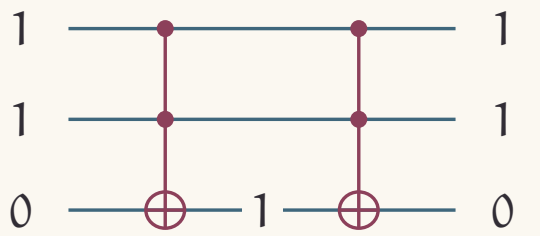
Infatti $ab\oplus ab = 0$ sia per $ab = 0$ sia per $ab = 1$; quindi $(t\oplus ab)\oplus ab = t\oplus 0 = t$. Per linearità, $T^2 = I_8$ e $T^{-1} = T$.

Per verificare l'unitarietà, calcoliamo

$$(T^\dagger T)_{jk} = \sum_{\ell=0}^{7} T^*_{\ell j} T_{\ell k}.$$

Ogni colonna ha un solo 1. Per $j = k$, la somma contiene $1\cdot 1$ e sette zeri: vale 1. Per $j \neq k$, i due 1 sono in righe diverse: ciascuno degli otto prodotti vale 0, dunque la somma vale 0.

$$T^\dagger T = I_8.$$



$110 \to 111 \to 110$. Con controlli inattivi: $100 \to 100 \to 100$.

La linearità permette ora di seguire separatamente i termini di una sovrapposizione. Cominciamo dal ruolo di un controllo fissato.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; $a,b,t\in\{0,1\}$. $\oplus$: XOR; $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$. I_8: identità 8×8, con 1 sulla diagonale e 0 altrove. $(T^\dagger)_{j\ell} = T^*_{\ell j}$; $j,k,\ell = 0,\dots,7$.

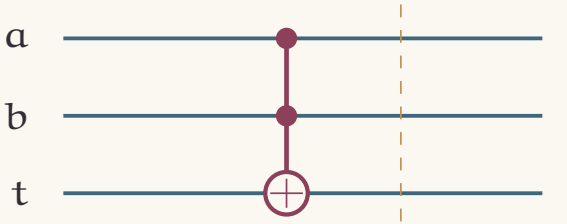
Un controllo fissato determina la porta restante

Fissiamo il primo controllo a e osserviamo la trasformazione degli altri due qubit. Per $a = 0$ il prodotto ab è sempre zero; per $a = 1$ coincide con b.

$$T|0, b, t\rangle = |0, b, t \oplus (0 \cdot b)\rangle = |0, b, t \oplus 0\rangle = |0, b, t\rangle,$$

$$T|1, b, t\rangle = |1, b, t \oplus (1 \cdot b)\rangle = |1, b, t \oplus b\rangle.$$

b	t	$t \oplus b$	uscita con $a = 1$
0	0	$0 \oplus 0 = 0$	100
0	1	$1 \oplus 0 = 1$	101
1	0	$0 \oplus 1 = 1$	111
1	1	$1 \oplus 1 = 0$	110



$a = 1 : \quad (b, t) \mapsto (b, t \oplus b)$

Con il primo controllo a uno, i due fili inferiori eseguono una CNOT. Con il primo controllo a zero, entrambi restano invariati.

Questa riduzione permette di prevedere gli esempi in sovrapposizione senza perdere il significato dei controlli.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Una sovrapposizione con controllo inattivo

Confrontiamo due ingressi che differiscono soltanto nel primo controllo. Cominciamo da $|\Psi\rangle = |0\rangle|+\rangle|0\rangle$, con $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$: il controllo fissato a zero deve mantenere inattiva la porta anche quando il secondo è in sovrapposizione. Espandiamo il prodotto perché Toffoli è definita sui vettori della base:

$$|\Psi\rangle = |0\rangle\frac{|0\rangle + |1\rangle}{\sqrt{2}}|0\rangle = \frac{|000\rangle + |010\rangle}{\sqrt{2}}, \qquad \|\Psi\|^2 = \tfrac{1}{2} + \tfrac{1}{2} = 1.$$

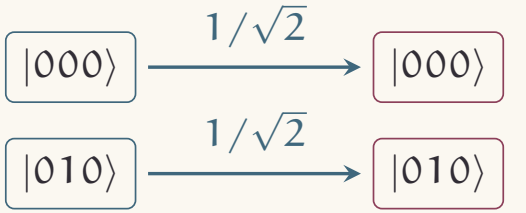
Entrambi i termini hanno $a = 0$. Calcoliamo le immagini:

$$T|000\rangle = |00, 0 \oplus (0 \cdot 0)\rangle = |000\rangle,$$

$$T|010\rangle = |01, 0 \oplus (0 \cdot 1)\rangle = |010\rangle.$$

Per linearità,

$$T|\Psi\rangle = \frac{T|000\rangle + T|010\rangle}{\sqrt{2}} = \frac{|000\rangle + |010\rangle}{\sqrt{2}} = |\Psi\rangle.$$



Ampiezze conservate nei due termini della stessa sovrapposizione.

Il controllo fissato a zero conserva lo stato. Attiviamo ora quel controllo mantenendo la stessa sovrapposizione sul secondo.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Attivare il controllo su una sovrapposizione

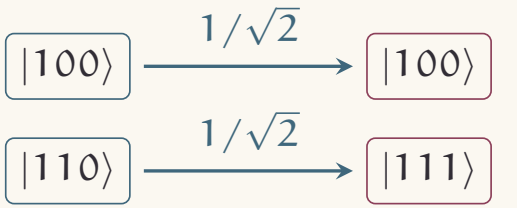
Cambiamo soltanto il primo controllo da zero a uno. Ora $|\Psi\rangle = |1\rangle|+\rangle|0\rangle = (|100\rangle + |110\rangle)/\sqrt{2}$, con norma quadrata $1/2 + 1/2 = 1$: Toffoli diventa una CNOT fra il secondo controllo e l'ausiliario. I prodotti dei controlli sono $1 \cdot 0 = 0$ e $1 \cdot 1 = 1$:

$$T|100\rangle = |10, 0 \oplus 0\rangle = |100\rangle, \qquad T|110\rangle = |11, 0 \oplus 1\rangle = |111\rangle.$$

La linearità conserva i coefficienti:

$$T|\Psi\rangle = \frac{T|100\rangle + T|110\rangle}{\sqrt{2}} = \frac{|100\rangle + |111\rangle}{\sqrt{2}} = |1\rangle \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Il primo qubit resta separato. I due inferiori formano la coppia di Bell, la cui mancata fattorizzazione è già stata dimostrata. Born dà $p(b = 0, t = 0) = p(b = 1, t = 1) = |1/\sqrt{2}|^2 = 1/2$; gli altri esiti hanno ampiezza e probabilità zero.



Ampiezze conservate nei due termini della stessa sovrapposizione.

Il primo controllo attiva una CNOT sui due qubit inferiori.

Gli esiti del secondo controllo e dell'ausiliario coincidono. Estendiamo l'ingresso alla sovrapposizione di entrambe le coppie di controlli.

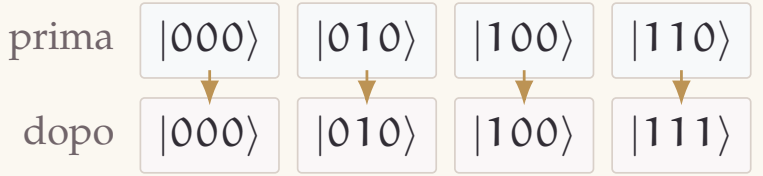
$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Applicare AND a una sovrapposizione

Per includere le quattro coppie con uguale ampiezza, prepariamo $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ sui controlli e $|0\rangle$ sull'ausiliario, che registrerà AND. Espandiamo lo stato per seguire i quattro contributi.

$$|\Psi_0\rangle = |+\rangle|+\rangle|0\rangle = \frac{(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes |0\rangle}{2} = \frac{|00\rangle \otimes |0\rangle + |01\rangle \otimes |0\rangle + |10\rangle \otimes |0\rangle + |11\rangle \otimes |0\rangle}{2}$$
$$= \frac{|000\rangle + |010\rangle + |100\rangle + |110\rangle}{2}.$$

$$T\frac{|000\rangle}{2} = \frac{|000\rangle}{2}, \quad T\frac{|010\rangle}{2} = \frac{|010\rangle}{2},$$
$$T\frac{|100\rangle}{2} = \frac{|100\rangle}{2}, \quad T\frac{|110\rangle}{2} = \frac{|111\rangle}{2}.$$



Ampiezze $1/2$ di un unico stato congiunto; gli altri termini restano fissi.

$$|\Psi_1\rangle = T|\Psi_0\rangle = \frac{|000\rangle + |010\rangle + |100\rangle + |111\rangle}{2} = \frac{1}{2}(1,0,1,0,1,0,0,1)^T.$$

La misura dell'ausiliario raggruppa tre contributi con AND zero e uno con AND uno.

DATI E REGOLE $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$; $T|a,b,t\rangle = |a,b,t \oplus ab\rangle$. Per 000, 010, 100: $ab = 0 \cdot 0 = 0$, $0 \cdot 1 = 0$, $1 \cdot 0 = 0$ e $0 \oplus 0 = 0$. Per 110: $ab = 1 \cdot 1 = 1$ e $0 \oplus 1 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$.

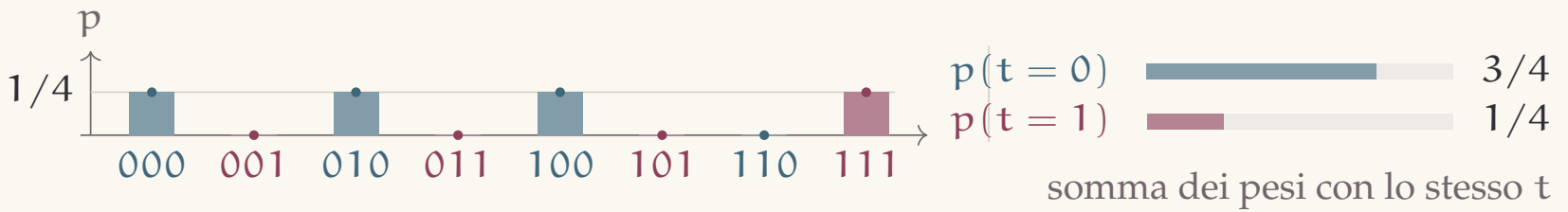
Probabilità di misura dell'ausiliario

Per $|\Psi_1\rangle = (1,0,1,0,1,0,0,1)^T/2$, nella base $000,\ldots,111$, prevediamo una misura eventuale: $p(a,b,t) = |c_{abt}|^2$. Le somme per ciascun valore di t danno la distribuzione dell'ausiliario.

abt	000	001	010	011	100	101	110	111
c_{abt}	$1/2$	0	$1/2$	0	$1/2$	0	0	$1/2$
$p(a,b,t)$	$(1/2)^2$	0^2	$(1/2)^2$	0^2	$(1/2)^2$	0^2	0^2	$(1/2)^2$
	$1/4$	0	$1/4$	0	$1/4$	0	0	$1/4$

La norma quadrata è $1/4+0+1/4+0+1/4+0+0+1/4 = 4/4 = 1$.

$$p(t=0) = p_{000}+p_{010}+p_{100}+p_{110} = 1/4+1/4+1/4+0 = 3/4,$$
$$p(t=1) = p_{001}+p_{011}+p_{101}+p_{111} = 0+0+0+1/4 = 1/4.$$



I tre contributi con AND zero danno probabilità $3/4$; quello con AND uno dà $1/4$. Riduciamo ora l'ingresso a due contributi, uno per ciascun valore di AND, e assegniamo loro pesi diversi.

DATI E REGOLE c_{abt}: ampiezza di $|abt\rangle$; $p(a,b,t) = |c_{abt}|^2$; $p(t) = \sum_{a,b} p(a,b,t)$. La base è ordinata $000,001,010,011,100,101,110,111$.

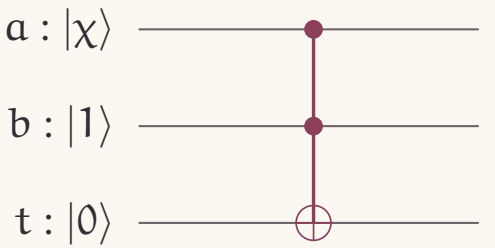
Scegliere due contributi con pesi diversi

Per studiare il peso del caso inattivo e di quello attivo, fissiamo il secondo controllo $b = 1$ e l'ausiliario $t = 0$. Il primo controllo è $|\chi\rangle = (3|0\rangle + 4|1\rangle)/5$; i numeri $3, 4, 5$ consentono una normalizzazione semplice.

Il prodotto rende esplicita la preparazione:

$$\begin{aligned} |\Psi\rangle &= \left(\frac{3}{5}|0\rangle + \frac{4}{5}|1\rangle\right) \otimes |1\rangle \otimes |0\rangle \\ &= \frac{3}{5}|0\rangle|1\rangle|0\rangle + \frac{4}{5}|1\rangle|1\rangle|0\rangle \\ &= \frac{3}{5}|010\rangle + \frac{4}{5}|110\rangle. \end{aligned}$$

$$\begin{aligned} \|\Psi\|^2 &= \left|\frac{3}{5}\right|^2 + \left|\frac{4}{5}\right|^2 = \frac{3^2}{5^2} + \frac{4^2}{5^2} \\ &= \frac{9}{25} + \frac{16}{25} = \frac{25}{25} = 1. \end{aligned}$$



$$t' = 0 \oplus (a \cdot 1) = a$$

Con $b = 1$, AND vale $ab = a \cdot 1 = a$. Il termine 010 è inattivo; 110 attiva lo scambio.

I due termini isolano il caso inattivo e quello attivo. Applichiamo ora Toffoli conservando le ampiezze assegnate.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$.

Trasferire i due pesi nei contributi di uscita

Ripartiamo da $|\Psi\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|110\rangle$, con $b = 1$ e $t = 0$. Toffoli conserva i controlli e aggiorna l'ausiliario con $t \oplus ab$, così il suo valore finale distingue i due casi.

Per il primo termine, $ab = 0 \cdot 1 = 0$:

$$T|010\rangle = |01, 0 \oplus 0\rangle = |010\rangle.$$

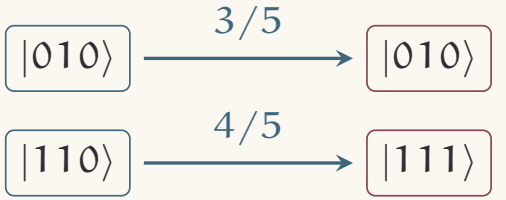
Per il secondo, $ab = 1 \cdot 1 = 1$:

$$T|110\rangle = |11, 0 \oplus 1\rangle = |111\rangle.$$

La linearità mantiene le ampiezze:

$$\begin{aligned} T|\Psi\rangle &= \frac{3}{5}T|010\rangle + \frac{4}{5}T|110\rangle \\ &= \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle. \end{aligned}$$

Il secondo contributo cambia posizione, conservando il coefficiente 4/5.



Ampiezze conservate nei due termini della stessa sovrapposizione.

L'ausiliario è correlato con il primo controllo. Born tradurrà le ampiezze conservate nei pesi dei due esiti.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$.

Dalle ampiezze alle probabilità dell'ausiliario

Lo stato dopo Toffoli è $|\Phi\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle$. I termini 010 e 111 provengono dai casi AND zero e AND uno: la misura dell'ausiliario ne leggerà i pesi.

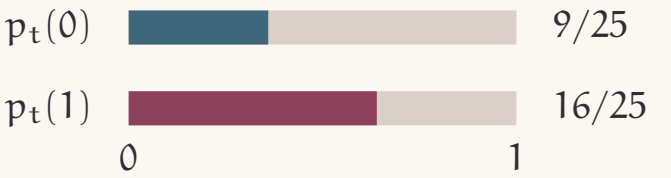
Applichiamo Born a ciascuna componente presente:

$$p(010) = \left|\frac{3}{5}\right|^2 = \frac{9}{25}, \qquad p(111) = \left|\frac{4}{5}\right|^2 = \frac{16}{25}.$$

Gli altri sei esiti hanno probabilità $|0|^2 = 0$. Sommando per terzo indice,

$$\begin{aligned} p_t(0) &= p(000) + p(010) + p(100) + p(110) \\ &= 0 + \frac{9}{25} + 0 + 0 = \frac{9}{25}, \\ p_t(1) &= 0 + 0 + 0 + \frac{16}{25} = \frac{16}{25}. \end{aligned}$$

Misura dell'ausiliario



$9/25 = 0{,}36$, $16/25 = 0{,}64$.

Il diagramma mostra probabilità; le ampiezze iniziali erano 3/5 e 4/5.

Un esito seleziona il caso inattivo (9/25) oppure quello attivo (16/25). Calcoliamo ora lo stato del ramo osservato.

$T|a,b,t\rangle = |a,b,t \oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $p(abt) = |c_{abt}|^2$; $p_t(j) = \sum_{a,b=0}^{1} |c_{abj}|^2$.

Condizionare lo stato all'esito 0 dell'ausiliario

Riprendiamo $|\Phi\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle$, ottenuto da $\frac{3}{5}|010\rangle + \frac{4}{5}|110\rangle$. Se la misura di t restituisce 0, selezioniamo le componenti con quel terzo indice mediante $P_0 = I_2 \otimes I_2 \otimes |0\rangle\langle 0|$.

$$P_0 = \mathrm{diag}(1,0,1,0,1,0,1,0).$$

Il proiettore seleziona il terzo indice:

$$P_0|010\rangle = 1|010\rangle, \quad P_0|111\rangle = 0|111\rangle.$$

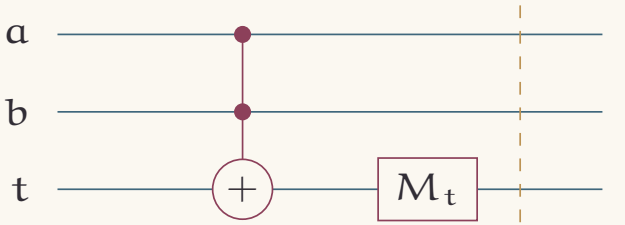
$$P_0|\Phi\rangle = (3/5)\cdot 1|010\rangle + (4/5)\cdot 0|111\rangle = (3/5)|010\rangle.$$

La norma quadrata fornisce la probabilità:

$$p_t(0) = \|P_0\Phi\|^2 = (3/5)^2 = 9/25.$$

Dividiamo per la radice di questo valore:

$$|\Phi_0\rangle = \frac{P_0|\Phi\rangle}{\sqrt{p_t(0)}} = \frac{(3/5)|010\rangle}{\sqrt{9/25}} = \frac{(3/5)|010\rangle}{3/5} = |010\rangle.$$



$|010\rangle = |01\rangle|0\rangle$

Dopo la misura selettiva, i controlli sono nello stato $|01\rangle$. Il risultato si riferisce alle esecuzioni con esito 0.

L'esito zero identifica 01 per questo ingresso. Con tutti i controlli possibili, AND zero ammette invece 00, 01 e 10.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000,001,010,011,100,101,110,111)$; $|abt\rangle = |a\rangle\otimes|b\rangle\otimes|t\rangle$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $I_2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$. Per $p>0$, stato successivo $P|\Phi\rangle/\sqrt{p}$. M_t: misura di t nella base $(|0\rangle,|1\rangle)$.

Condizionare lo stato all'esito 1 dell'ausiliario

Riprendiamo $|\Phi\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle$, ottenuto da $\frac{3}{5}|010\rangle + \frac{4}{5}|110\rangle$. Se la misura di t restituisce 1, selezioniamo le componenti con quel terzo indice mediante $P_1 = I_2 \otimes I_2 \otimes |1\rangle\langle 1|$.

$$P_1 = \mathrm{diag}(0,1,0,1,0,1,0,1).$$

Il proiettore seleziona il terzo indice:

$$P_1|010\rangle = 0|010\rangle, \quad P_1|111\rangle = 1|111\rangle.$$

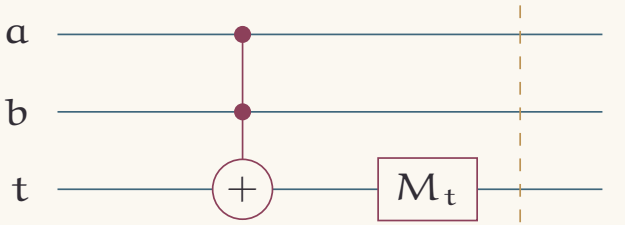
$$P_1|\Phi\rangle = (3/5)\cdot 0|010\rangle + (4/5)\cdot 1|111\rangle = (4/5)|111\rangle.$$

La norma quadrata fornisce la probabilità:

$$p_t(1) = \|P_1\Phi\|^2 = (4/5)^2 = 16/25.$$

Dividiamo per la radice di questo valore:

$$|\Phi_1\rangle = \frac{P_1|\Phi\rangle}{\sqrt{p_t(1)}} = \frac{(4/5)|111\rangle}{\sqrt{16/25}} = \frac{(4/5)|111\rangle}{4/5} = |111\rangle.$$



$|111\rangle = |11\rangle|1\rangle$

Dopo la misura selettiva, i controlli sono nello stato $|11\rangle$. Il risultato si riferisce alle esecuzioni con esito 1.

L'esito uno identifica 11 e ha peso 16/25. Confrontiamo ora stati con gli stessi moduli e una fase relativa diversa.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000,001,010,011,100,101,110,111)$; $|abt\rangle = |a\rangle\otimes|b\rangle\otimes|t\rangle$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $I_2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$. Per $p>0$, stato successivo $P|\Phi\rangle/\sqrt{p}$. M_t: misura di t nella base $(|0\rangle,|1\rangle)$.

Trasformare un'ampiezza complessa con Toffoli

Per separare il ruolo della fase da quello dei pesi, moltiplichiamo per i soltanto la seconda ampiezza: $|\Psi\rangle = \frac{3}{5}|010\rangle + \frac{4i}{5}|110\rangle$. La fase relativa aumenta di $\pi/2$ e i moduli restano uguali. Con $i^2 = -1$ e $i^* = -i$, verifichiamo:

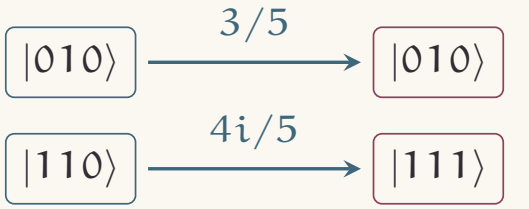
$$\left|\frac{4i}{5}\right|^2 = \frac{(-4i)(4i)}{25} = \frac{-16i^2}{25} = \frac{16}{25}, \qquad \|\Psi\|^2 = \frac{9}{25} + \frac{16}{25} = 1.$$

Le immagini della base restano

$$T|010\rangle = |01, 0 \oplus (0 \cdot 1)\rangle = |010\rangle,$$
$$T|110\rangle = |11, 0 \oplus (1 \cdot 1)\rangle = |111\rangle.$$

Per linearità,

$$T|\Psi\rangle = \frac{3}{5}T|010\rangle + \frac{4i}{5}T|110\rangle = \frac{3}{5}|010\rangle + \frac{4i}{5}|111\rangle.$$



Ampiezze conservate nei due termini della stessa sovrapposizione.

Il coefficiente complesso resta associato al termine trasformato. Confrontiamo la misura con quella dello stato a coefficienti reali.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $|z|^2 = z^* z$; $i^2 = -1$, $i^* = -i$.

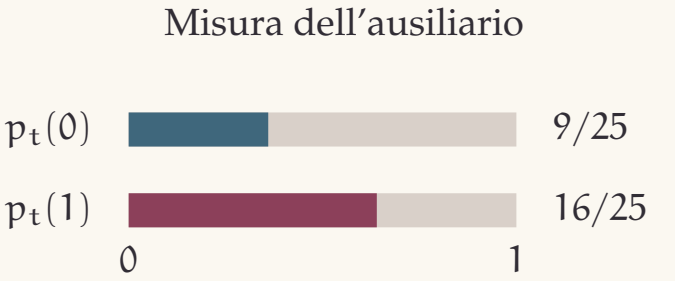
Confrontare ampiezze reali e complesse nella misura

Confrontiamo le uscite $|\Phi_R\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle$ e $|\Phi_C\rangle = \frac{3}{5}|010\rangle + \frac{4i}{5}|111\rangle$. La misura dell'ausiliario usa soltanto i moduli quadrati delle componenti.

$$p_{t,R}(0) = \frac{3\cdot 3}{25} = \frac{9}{25}, \quad p_{t,R}(1) = \frac{4\cdot 4}{25} = \frac{16}{25},$$

$$p_{t,C}(0) = \frac{9}{25}, \quad p_{t,C}(1) = \frac{(-4i)(4i)}{25} = \frac{-16i^2}{25} = \frac{16}{25}.$$

Tutte le componenti omesse sono nulle. In entrambi i casi $p_t(0) + p_t(1) = 25/25 = 1$.
I due stati hanno una fase relativa diversa: il rapporto fra le due ampiezze è $4/3$ nel primo caso e $4i/3$ nel secondo.



La stessa distribuzione può essere associata a stati differenti.

La variazione della sola fase conserva questa distribuzione computazionale. Per distinguerla occorre una successiva ricombinazione delle ampiezze: è il procedimento che useremo in Deutsch.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; a, b: controlli, t: ausiliario. Base $(000,001,010,011,100,101,110,111)$; $|abt\rangle = |a\rangle\otimes|b\rangle\otimes|t\rangle$. $|z|^2 = z^*z$; $i^2 = -1$, $i^* = -i$; $p_t(j) = \sum_{a,b}|c_{abj}|^2$.

Il problema: classificare una funzione ignota

Un dispositivo realizza una funzione fissata $f : \{0,1\} \to \{0,1\}$. Possiamo interrogarlo scegliendo un ingresso. Dobbiamo stabilire con certezza se i due valori siano uguali oppure diversi. Le possibilità sono quattro:

$f(x)$	$f(0)$	$f(1)$	$d = f(0) \oplus f(1)$	classe
0	0	0	$0 \oplus 0 = 0$	costante
x	0	1	$0 \oplus 1 = 1$	bilanciata
1	1	1	$1 \oplus 1 = 0$	costante
$1 \oplus x$	1	0	$1 \oplus 0 = 1$	bilanciata

La tabella descrive tutte le funzioni compatibili con il problema; il nostro compito consiste nel determinarne la classe attraverso le risposte del dispositivo. Durante l'esecuzione il dispositivo usa una sola di queste funzioni, la cui identità rimane ignota. Il bit d riassume la classificazione richiesta.

Il confronto classico determina i due valori e calcola il loro XOR. Cominciamo da questa procedura.

$\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $f : \{0,1\} \to \{0,1\}$; $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. Il costo conta le interrogazioni necessarie a una risposta certa.

Due interrogazioni classiche determinano la classe

Interroghiamo il dispositivo su 0 e su 1, poi calcoliamo lo XOR delle risposte. Per esempio, se osserviamo $f(0) = 0$ e $f(1) = 1$, otteniamo $d = 0 \oplus 1 = 1$: la funzione è bilanciata.

Una sola interrogazione lascia invece due classi compatibili, qualunque siano l'ingresso e la risposta:

x	$f(x)$ osservato	$(f(0), f(1))$ costante	$(f(0), f(1))$ bilanciata
0	0	$(0,0)$	$(0,1)$
0	1	$(1,1)$	$(1,0)$
1	0	$(0,0)$	$(1,0)$
1	1	$(1,1)$	$(0,1)$

In ogni riga restano una funzione con $d = 0$ e una con $d = 1$. Una procedura classica sempre corretta richiede quindi due interrogazioni. Per cercare una procedura quantistica, definiamo ora una porta che rappresenti la funzione e che possa agire coerentemente su una sovrapposizione.

La procedura esatta richiede due interrogazioni. La porta seguente permette di applicare la funzione a uno stato in sovrapposizione.

$\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $f : \{0,1\} \to \{0,1\}$; $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. Il costo conta le interrogazioni necessarie a una risposta certa.

Definire il compito dei due registri

La procedura classica determina $f(0)$ e $f(1)$ separatamente. Per costruire quella quantistica definiamo una porta U_f, accessibile all'algoritmo, che realizza una funzione fissata nel dispositivo e ancora ignota. Prepariamo due qubit: A rappresenta l'argomento x; B contiene il valore ausiliario y, scelto prima dell'interrogazione.

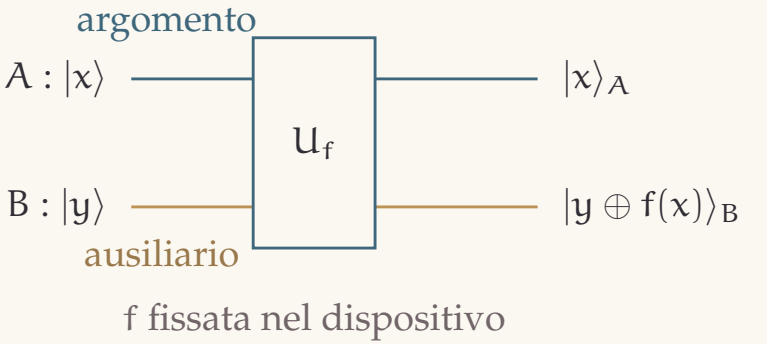
Per un ingresso della base, la regola è

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

L'etichetta x viene conservata; il valore $f(x)$ viene combinato con y mediante XOR. Preparando B in zero, otteniamo

$$U_f|x0\rangle = |x, 0 \oplus f(x)\rangle = |x, f(x)\rangle.$$

Con B in uno, l'uscita contiene $1 \oplus f(x)$, cioè il complemento di $f(x)$. Il significato dell'ausiliario dipende quindi dalla sua preparazione.



x è l'argomento; f è fissata nel dispositivo.

Conservare x mantiene distinguibili gli ingressi anche per una funzione costante. La scelta dello XOR rende reversibile anche l'aggiornamento di B; verifichiamo questa proprietà.

A: argomento; B: ausiliario. $x, y \in \{0,1\}$; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Lo XOR rende reversibile l'aggiornamento

Quando $f(x) = 0$, lo XOR conserva y; quando $f(x) = 1$, lo inverte. Le due azioni sono rispettivamente I_2 e X. L'esponente seleziona il caso:

$$U_f|x\rangle_A|y\rangle_B = |x\rangle_A \otimes X^{f(x)}|y\rangle_B, \qquad X^0 = I_2, \quad X^1 = X.$$

Le quattro possibilità sono:

$f(x)$	y	$y \oplus f(x)$	porta su B
0	0	$0 \oplus 0 = 0$	I_2
0	1	$1 \oplus 0 = 1$	I_2
1	0	$0 \oplus 1 = 1$	X
1	1	$1 \oplus 1 = 0$	X

U_f agisce su entrambi i qubit. Il fattore $X^{f(x)}$ descrive l'azione su B per ciascun ingresso di base.

La funzione resta la stessa nelle due applicazioni. Il secondo XOR annulla il primo:

$$\begin{aligned} U_f^2|x,y\rangle &= U_f|x, y \oplus f(x)\rangle \\ &= |x, (y \oplus f(x)) \oplus f(x)\rangle \\ &= |x, y \oplus (f(x) \oplus f(x))\rangle \\ &= |x, y \oplus 0\rangle = |x, y\rangle. \end{aligned}$$

Si recupera l'ingresso: $U_f^{-1} = U_f$. La porta permuta la base ortonormale; è quindi unitaria.

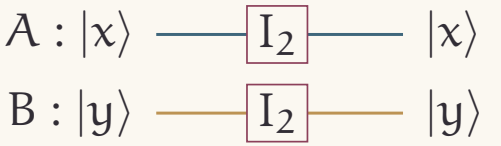
Per una sovrapposizione applichiamo la regola per linearità, conservando i coefficienti. Individuiamo ora i circuiti corrispondenti alle quattro funzioni.

$x, y, f(x) \in \{0, 1\}$; $|x, y\rangle = |x\rangle_A \otimes |y\rangle_B$. Lo XOR è associativo e $z \oplus z = 0$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$.

Realizzare le due funzioni costanti

Per una funzione costante, l'operazione su B è indipendente da A: la costante zero conserva B, la costante uno lo inverte sempre. Verifichiamo $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$ sui quattro ingressi.

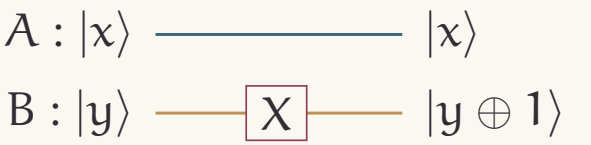
$f(x) = 0: \quad U_f = I_4 = I_2 \otimes I_2.$



$$U_f|00\rangle = |0, 0 \oplus 0\rangle = |00\rangle,$$
$$U_f|01\rangle = |0, 1 \oplus 0\rangle = |01\rangle,$$
$$U_f|10\rangle = |1, 0 \oplus 0\rangle = |10\rangle,$$
$$U_f|11\rangle = |1, 1 \oplus 0\rangle = |11\rangle.$$

Tutti e quattro gli ingressi restano invariati.

$f(x) = 1: \quad U_f = I_2 \otimes X.$



$$U_f|00\rangle = |0, 0 \oplus 1\rangle = |01\rangle,$$
$$U_f|01\rangle = |0, 1 \oplus 1\rangle = |00\rangle,$$
$$U_f|10\rangle = |1, 0 \oplus 1\rangle = |11\rangle,$$
$$U_f|11\rangle = |1, 1 \oplus 1\rangle = |10\rangle.$$

Con $y = 1$, l'inversione riporta B a zero.

Nei casi costanti il bersaglio subisce la stessa operazione per entrambi gli argomenti. Passiamo alla funzione identità, che fa dipendere l'inversione da x.

$|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; I_4: identità sulle quattro componenti. $I_2 \otimes X$ applica X soltanto a B.

La funzione identità produce una CNOT

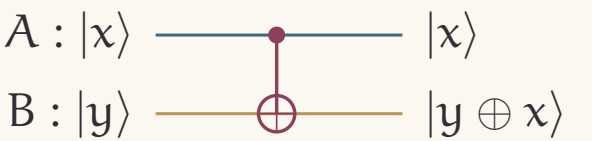
Consideriamo $f(x) = x$: il dispositivo restituisce il proprio argomento. Il valore che decide l'inversione coincide quindi con il bit di A. Se $x = 0$, B conserva il proprio valore; se $x = 1$, B viene invertito. Questa dipendenza è esattamente quella della CNOT, con A come controllo e B come bersaglio.

Sostituiamo $f(0) = 0$ e $f(1) = 1$ nella definizione:

$$U_f|00\rangle = |0, 0 \oplus f(0)\rangle = |0, 0 \oplus 0\rangle = |00\rangle,$$
$$U_f|01\rangle = |0, 1 \oplus f(0)\rangle = |0, 1 \oplus 0\rangle = |01\rangle,$$
$$U_f|10\rangle = |1, 0 \oplus f(1)\rangle = |1, 0 \oplus 1\rangle = |11\rangle,$$
$$U_f|11\rangle = |1, 1 \oplus f(1)\rangle = |1, 1 \oplus 1\rangle = |10\rangle.$$

Le prime due immagini conservano B; le ultime due scambiano $|10\rangle$ e $|11\rangle$. Ne segue

$$U_f|x, y\rangle = |x, y \oplus x\rangle, \qquad U_f = \mathrm{CNOT}_{A\to B}.$$



Il punto sul filo A indica il controllo. Il simbolo sul filo B inverte il bersaglio quando il controllo vale uno.

Le quattro righe verificano tutti gli ingressi della base.

Per l'identità l'inversione è associata a x=1. La funzione complementare scambierà questa condizione: il suo valore sarà uno quando x=0.

A: argomento; B: ausiliario. $x, y \in \{0, 1\}$; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$; base $(00, 01, 10, 11)$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Il complemento richiede CNOT seguita da X

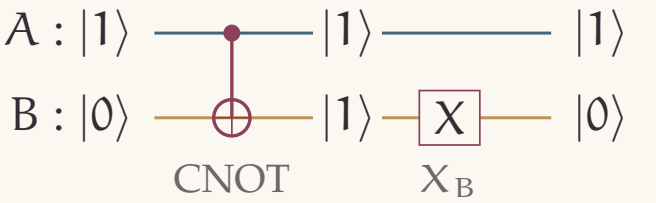
Per $f(x) = 1 \oplus x$ si ha $f(0) = 1 \oplus 0 = 1$ e $f(1) = 1 \oplus 1 = 0$. Otteniamo l'uscita combinando prima y con x mediante CNOT, poi invertendo il risultato con X su B:

$$y \oplus f(x) = y \oplus (1 \oplus x) = y \oplus (x \oplus 1) = (y \oplus x) \oplus 1, \qquad U_f = (I_2 \otimes X)\,\mathrm{CNOT}_{A\to B}.$$

Il circuito si esegue da sinistra a destra; nel prodotto di operatori agisce per prima la CNOT a destra.

ingresso	dopo CNOT	dopo X_B
$\lvert 00\rangle$	$\lvert 0, 0 \oplus 0\rangle = \lvert 00\rangle$	$\lvert 0, 0 \oplus 1\rangle = \lvert 01\rangle$
$\lvert 01\rangle$	$\lvert 0, 1 \oplus 0\rangle = \lvert 01\rangle$	$\lvert 0, 1 \oplus 1\rangle = \lvert 00\rangle$
$\lvert 10\rangle$	$\lvert 1, 0 \oplus 1\rangle = \lvert 11\rangle$	$\lvert 1, 1 \oplus 1\rangle = \lvert 10\rangle$
$\lvert 11\rangle$	$\lvert 1, 1 \oplus 1\rangle = \lvert 10\rangle$	$\lvert 1, 0 \oplus 1\rangle = \lvert 11\rangle$

L'uscita inverte B per $x = 0$ e lo conserva per $x = 1$, come richiedono $f(0) = 1$ e $f(1) = 0$.



Scegliamo $|10\rangle$ per seguire le due inversioni. Il bersaglio passa da zero a uno e poi torna a zero, coerentemente con $f(1) = 0$.

Le quattro realizzazioni descrivono i dispositivi possibili. Durante l'algoritmo la funzione resta ignota: costruiamo ora un unico schema di preparazione e lettura valido per tutti i casi.

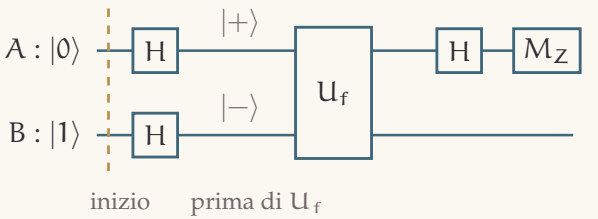
A: controllo x; B: bersaglio y; $|xy\rangle = |x\rangle_A \otimes |y\rangle_B$. $X_B = I_2 \otimes X$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. CNOT: $|x, y\rangle \mapsto |x, y \oplus x\rangle$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$.

Seguire il circuito dalla preparazione alla misura

L'algoritmo riceve accesso a un oracolo la cui funzione resta ignota. Usiamo lo stesso circuito esterno nei quattro casi, inserendo una sola chiamata a U_f fra preparazione e lettura. All'inizio poniamo A in $|0\rangle$ e B in $|1\rangle$; le due Hadamard preparano gli stati che raggiungono l'oracolo. Indichiamo ogni sezione mediante lo stato congiunto:

$$
\begin{aligned}
|\psi_0\rangle &= |0\rangle|1\rangle, \\
|\psi_1\rangle &= (H \otimes H)|\psi_0\rangle, \\
|\psi_2\rangle &= U_f|\psi_1\rangle, \\
|\psi_3\rangle &= (H \otimes I_2)|\psi_2\rangle.
\end{aligned}
$$

Calcoleremo gli stati in questo ordine. Le due linee del circuito indicano i registri; il vettore a due qubit descrive lo stato congiunto in ogni tappa.



Stato alla sezione

$|\psi_0\rangle = |0\rangle|1\rangle$

I valori $|0\rangle$ e $|1\rangle$ sono gli ingressi iniziali. Le etichette $|+\rangle$ e $|-\rangle$ indicano gli stati immediatamente prima di U_f.

La preparazione viene scelta per trasformare i valori della funzione in segni che la Hadamard finale possa combinare.

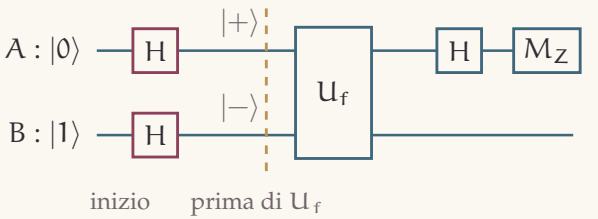
A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$: identità sul secondo qubit.

Preparare le ampiezze e i segni dei due qubit

Il circuito parte da $|\psi_0\rangle = |0\rangle_A|1\rangle_B$. Per conoscere gli ingressi effettivi dell'oracolo, calcoliamo le due Hadamard separatamente, poiché ciascuna agisce su uno dei fattori. I prodotti di riga determinano i coefficienti di ciascun qubit:

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

Abbiamo ottenuto $|+\rangle$ per A e $|-\rangle$ per B. Costruiamo ora il vettore congiunto, che costituisce l'ingresso effettivo dell'oracolo.



Stato alla sezione

$$|\psi_1\rangle = |+\rangle_A|-\rangle_B$$

A entra nell'oracolo in $|+\rangle$, B in $|-\rangle$. Il segno opposto delle ampiezze di B farà dipendere dallo scambio un fattore -1.

I due prodotti determinano gli stati dei singoli registri. La continuazione ne sviluppa il prodotto tensoriale.

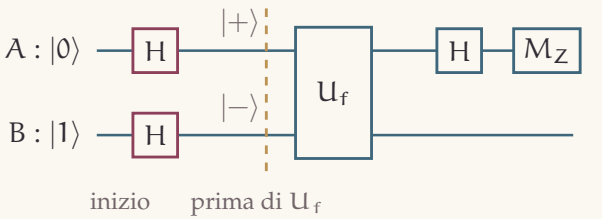
A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Costruire lo stato che entra nell'oracolo

Le due Hadamard hanno dato $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Poiché l'ingresso è un prodotto, l'azione congiunta si ricompone attraverso il prodotto tensoriale:

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

Il coefficiente comune è $(1/\sqrt{2})(1/\sqrt{2}) = 1/2$. I registri arrivano dunque all'oracolo in $|+\rangle_A|-\rangle_B$: il primo fornisce i contributi dei due argomenti, il secondo prepara ampiezze di segno opposto.



Stato alla sezione

$|\psi_1\rangle = |+\rangle_A|-\rangle_B$

La sezione precede U_f. La normalizzazione di ciascun fattore è $(1^2 + 1^2)/2 = 1$; il prodotto ha norma uno.

Espandiamo ora il prodotto nella base congiunta, così da applicare la definizione dell'oracolo a ogni termine.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

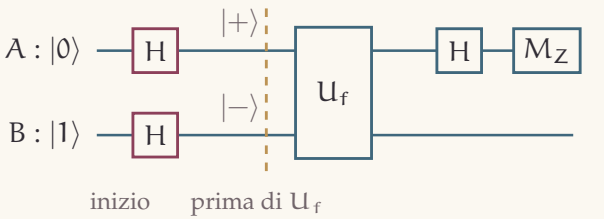
Espandere lo stato per applicare la definizione

L'oracolo riceve $|+\rangle_A|-\rangle_B$. La sua definizione è scritta sui vettori della base, quindi espandiamo il prodotto in quattro termini ai quali applicare la stessa regola. La distribuzione conserva sia le ampiezze sia i segni della preparazione:

$$\begin{aligned}|\psi_1\rangle &= \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) \\ &= \frac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle) \\ &= \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle).\end{aligned}$$

La linearità consente di trasformare separatamente questi quattro vettori, mantenendo i coefficienti:

$$|\psi_2\rangle = \frac{1}{2}\big(U_f|00\rangle - U_f|01\rangle + U_f|10\rangle - U_f|11\rangle\big).$$



Stato alla sezione

$$|\psi_1\rangle = \frac{|00\rangle - |01\rangle + |10\rangle - |11\rangle}{2}$$

Calcoliamo ora le quattro immagini senza assegnare ancora valori specifici alla funzione.

La norma quadrata è $4 \cdot |1/2|^2 = 4/4 = 1$; i segni modificano le ampiezze mantenendo questa norma.

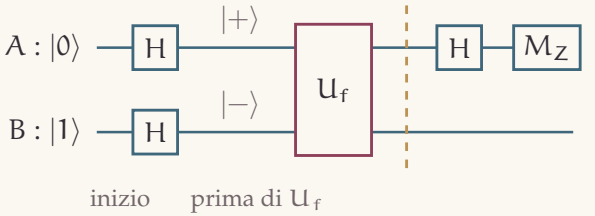
A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Applicare l'oracolo a ciascun ingresso della base

La preparazione ha dato $|\psi_1\rangle = (|00\rangle - |01\rangle + |10\rangle - |11\rangle)/2$. Per trasformarla usiamo $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$: il primo indice seleziona il valore della funzione e il secondo entra nello XOR. Sostituiamo le quattro coppie:

$$U_f|00\rangle = |0\rangle|f(0) \oplus 0\rangle,$$
$$U_f|01\rangle = |0\rangle|f(0) \oplus 1\rangle,$$
$$U_f|10\rangle = |1\rangle|f(1) \oplus 0\rangle,$$
$$U_f|11\rangle = |1\rangle|f(1) \oplus 1\rangle.$$

Il primo indice determina quale valore della funzione interviene. Il secondo indice determina il bit con cui quel valore viene combinato. Inseriamo queste immagini nella combinazione lineare, conservando i due segni meno della preparazione.



Stato alla sezione

$|\psi_2\rangle = U_f|\psi_1\rangle$

Le quattro righe sono il calcolo lineare di una sola trasformazione. Il dispositivo viene applicato una volta allo stato congiunto.
Lo XOR è commutativo:
$y \oplus f(x) = f(x) \oplus y$.

Le quattro sostituzioni descrivono i contributi di una sola chiamata coerente all'oracolo.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Ricomporre i contributi dopo l'oracolo

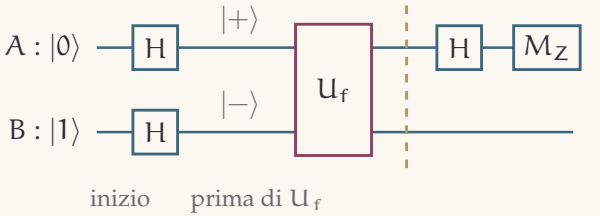
Le quattro immagini appena calcolate devono ora essere ricomposte con i coefficienti della preparazione. Riprendiamo dunque l'azione dell'oracolo sullo stato completo:

$$|\psi_2\rangle = \tfrac{1}{2}(U_f|00\rangle - U_f|01\rangle + U_f|10\rangle - U_f|11\rangle).$$

Sostituiamo le quattro immagini e raccogliamo i termini che hanno lo stesso primo indice:

$$|\psi_2\rangle = \frac{1}{2}\Big[|0\rangle\big(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle\big) + |1\rangle\big(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle\big)\Big].$$

Questa espressione mantiene distinti i contributi associati a 0 e a 1. Per semplificarla, calcoleremo la differenza fra i due vettori dell'ausiliario per ciascun possibile valore della funzione.



Stato alla sezione

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

La sezione è dopo l'oracolo. Stiamo riscrivendo lo stato ottenuto, senza aggiungere porte.

Le parentesi dell'ausiliario hanno la stessa struttura; cambia il valore $f(0)$ oppure $f(1)$.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Ricavare il segno associato al valore della funzione

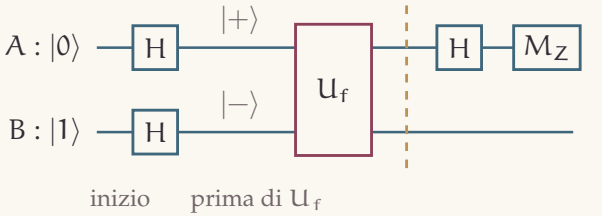
Nell'uscita dell'oracolo compare la differenza $|b \oplus 0\rangle - |b \oplus 1\rangle$, con $b = f(0)$ oppure $b = f(1)$. Per comprendere il ruolo del segno iniziale dell'ausiliario, calcoliamo questa differenza per i due valori possibili di b:

$$\begin{aligned} b = 0: \quad & |0 \oplus 0\rangle - |0 \oplus 1\rangle = |0\rangle - |1\rangle, \\ b = 1: \quad & |1 \oplus 0\rangle - |1 \oplus 1\rangle = |1\rangle - |0\rangle \\ & \qquad\qquad = -(|0\rangle - |1\rangle). \end{aligned}$$

Il secondo caso scambia l'ordine dei due termini, perciò introduce un segno meno. Poiché $(-1)^0 = 1$ e $(-1)^1 = -1$, le due uguaglianze si scrivono insieme:

$$|b \oplus 0\rangle - |b \oplus 1\rangle = (-1)^b (|0\rangle - |1\rangle).$$

Useremo questa identità per $b = f(0)$ e per $b = f(1)$.



Stato alla sezione

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

L'oracolo produce il segno; questa slide ne sviluppa il calcolo sui due valori possibili.

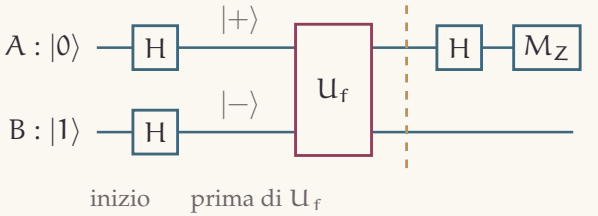
Il simbolo b indica qui il valore della funzione ed è distinto dal nome B del registro ausiliario.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Sostituire i due segni nello stato congiunto

La differenza dei due vettori dell'ausiliario equivale a $(-1)^b(|0\rangle - |1\rangle)$. Inseriamo questo risultato nello stato congiunto, prima con $b = f(0)$ e poi con $b = f(1)$. In questo modo ogni valore della funzione diventa un coefficiente di segno:

$$
\begin{aligned}
|\psi_2\rangle = \frac{1}{2}\Big[&|0\rangle\big(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle\big) \\
&+|1\rangle\big(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle\big)\Big] \\
= \frac{1}{2}\Big[&(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) \\
&+(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)\Big].
\end{aligned}
$$



Stato alla sezione

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

Il valore della funzione compare ora nel coefficiente di ciascun contributo. Il vettore dell'ausiliario è identico nei due termini, quindi può essere raccolto mediante la distributività del prodotto tensoriale.

Il passaggio conserva tutte le ampiezze e rende visibile il fattore che raccoglieremo nella slide successiva.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x)\oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Separare il segno comune dai due coefficienti

Raccogliamo il vettore comune dell'ausiliario, $|0\rangle - |1\rangle$, per confrontare i coefficienti di A:

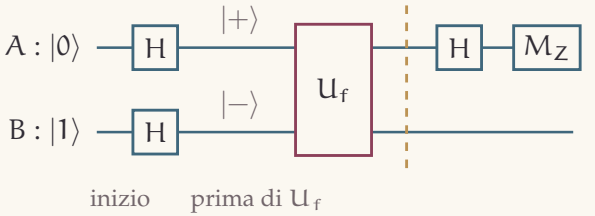
$$|\psi_2\rangle = \frac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle).$$

Il secondo coefficiente, diviso per il segno raccolto, diventa

$$\frac{(-1)^{f(1)}}{(-1)^{f(0)}} = (-1)^{f(1)}(-1)^{f(0)}.$$

Le quattro coppie verificano che questo prodotto dipende dallo XOR:

$f(0)$	$f(1)$	$(-1)^{f(0)}(-1)^{f(1)}$	$(-1)^{f(0)\oplus f(1)}$
0	0	$1 \cdot 1 = 1$	$(-1)^0 = 1$
0	1	$1 \cdot (-1) = -1$	$(-1)^1 = -1$
1	0	$(-1) \cdot 1 = -1$	$(-1)^1 = -1$
1	1	$(-1)(-1) = 1$	$(-1)^0 = 1$



Stato alla sezione

$$|\psi_2\rangle = U_f|\psi_1\rangle$$

Per raccogliere anche $(-1)^{f(0)}$, dividiamo il secondo coefficiente per questo segno. Un numero uguale a $+1$ o -1 coincide con il proprio inverso. Il rapporto calcolato a sinistra usa questa proprietà.

La tabella giustifica la sostituzione del prodotto dei segni con $(-1)^{f(0)\oplus f(1)}$.

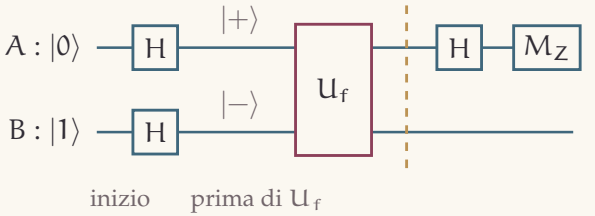
A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Isolare il segno che contiene la classificazione

Usiamo il rapporto dei segni appena calcolato per raccogliere $(-1)^{f(0)}$. Manteniamo espliciti entrambi i fattori dello stato:

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{2}\left[(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle\right](|0\rangle - |1\rangle) \\ &= \frac{(-1)^{f(0)}}{2}\left[|0\rangle + \frac{(-1)^{f(1)}}{(-1)^{f(0)}}|1\rangle\right](|0\rangle - |1\rangle) \\ &= (-1)^{f(0)}\frac{1}{2}\left[|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\right](|0\rangle - |1\rangle).\end{aligned}$$

Poniamo $d = f(0) \oplus f(1)$ e distribuiamo $1/2 = (1/\sqrt{2})(1/\sqrt{2})$ fra i due fattori. I due stati normalizzati sono indicati accanto al circuito; A contiene il segno relativo della classificazione.



$$|\phi\rangle_A = \frac{|0\rangle + (-1)^d|1\rangle}{\sqrt{2}},$$

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

$$|\psi_2\rangle = (-1)^{f(0)}|\phi\rangle_A \otimes |-\rangle_B.$$

La fase globale ha modulo quadro $|(-1)^{f(0)}|^2 = 1$ e conserva le probabilità.

Lo stato è fattorizzato: (H su A) e identità su B trasformano il primo fattore e conservano il secondo.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente. La norma quadrata di ciascun fattore è $(1^2 + 1^2)/2 = 1$. $(H \otimes I)(|\phi\rangle \otimes |-\rangle) = H|\phi\rangle \otimes |-\rangle$.

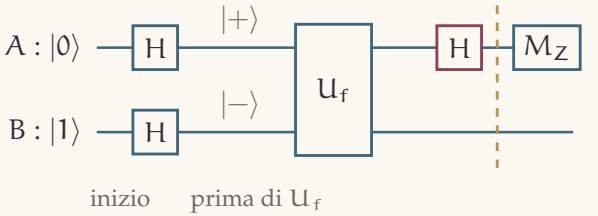
Espandere l'azione dell'ultima Hadamard

Per rendere osservabile il segno relativo applichiamo la Hadamard al fattore $|\phi\rangle = (|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle)/\sqrt{2}$. La linearità permette di trasformare ciascun vettore della base mantenendo il suo coefficiente:

$$H|\phi\rangle = \frac{1}{\sqrt{2}}\left(H|0\rangle + (-1)^{f(0)\oplus f(1)}H|1\rangle\right).$$

Sostituiamo $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, poi distribuiamo:

$$H|\phi\rangle = \frac{1}{2}\Big(|0\rangle + |1\rangle + (-1)^{f(0)\oplus f(1)}|0\rangle - (-1)^{f(0)\oplus f(1)}|1\rangle\Big).$$



Prima di H,
$p_A(0) = |1/\sqrt{2}|^2 = 1/2$,
$p_A(1) = |(-1)^d/\sqrt{2}|^2 = 1/2$.
La misura diretta dà gli stessi pesi per entrambe le classi. H combina i segni e rende diversi gli esiti finali.

$1/2 = (1/\sqrt{2})(1/\sqrt{2})$. Sommiamo i contributi che accompagnano lo stesso vettore della base.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente. $\oplus$: XOR; $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$.

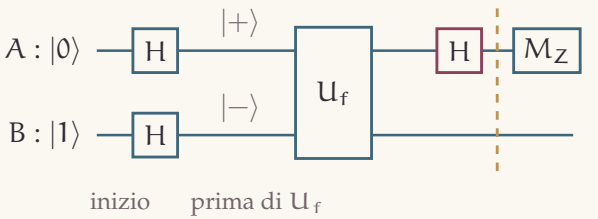
Raccogliere le ampiezze dei due possibili esiti

La Hadamard ha prodotto due contributi per ciascun esito. Per ricavarne le probabilità dobbiamo prima sommare le ampiezze che accompagnano lo stesso vettore. Riprendiamo l'espansione, con $d = f(0) \oplus f(1)$:

$$H|\phi\rangle = \tfrac{1}{2}\big(|0\rangle + |1\rangle + (-1)^d|0\rangle - (-1)^d|1\rangle\big).$$

I termini che moltiplicano lo stesso vettore contribuiscono alla stessa ampiezza. Raccogliendo prima $|0\rangle$ e poi $|1\rangle$ otteniamo

$$H|\phi\rangle = \frac{1}{2}\Big[\big(1 + (-1)^{f(0)\oplus f(1)}\big)|0\rangle + \big(1 - (-1)^{f(0)\oplus f(1)}\big)|1\rangle\Big].$$



Stato alla sezione

$$|\psi_3\rangle = (-1)^{f(0)} H|\phi\rangle_A |-\rangle_B$$

La prima ampiezza somma i due segni; la seconda ne calcola la differenza. Sostituiremo $d = 0$ e $d = 1$ per individuare l'esito che conserva ampiezza.

Il circuito ha trasformato la fase relativa in ampiezze differenti per gli esiti della misura.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $|0\rangle = (1,0)^\top$, $|1\rangle = (0,1)^\top$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Leggere zero per le funzioni costanti

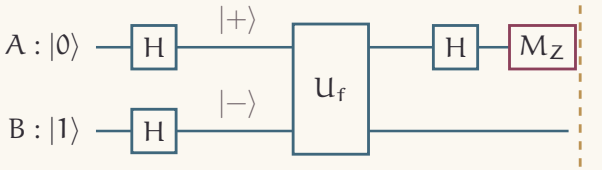
Per una funzione costante i due valori coincidono, dunque $d = f(0) \oplus f(1) = 0$ e $(-1)^d = 1$. Sostituiamo questo segno nelle ampiezze finali: la loro somma e la loro differenza stabiliscono quali esiti possono essere osservati.

$$c_0 = \frac{1 + (1)}{2} = 2/2 = 1, \qquad c_1 = \frac{1 - (1)}{2} = 0/2 = 0.$$

Quindi $H|\phi\rangle = 1|0\rangle + 0|1\rangle = |0\rangle$. La regola di Born fornisce

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

La probabilità totale è $1 + 0 = 1$. La misura restituisce con certezza 0, che coincide con la classificazione cercata. Il fattore globale $(-1)^{f(0)}$ conserva questi pesi.



Stato alla sezione

$$|\psi_3\rangle = (-1)^{f(0)}|0\rangle_A|-\rangle_B$$

La misura legge A nella base computazionale. Il secondo qubit resta nello stesso fattore.

La differenza delle ampiezze si annulla; l'altro esito raccoglie probabilità uno.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $p_A(j) = |c_j|^2$ per $c_0|0\rangle + c_1|1\rangle$ normalizzato; $|z|^2 = z^*z$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Leggere uno per le funzioni bilanciate

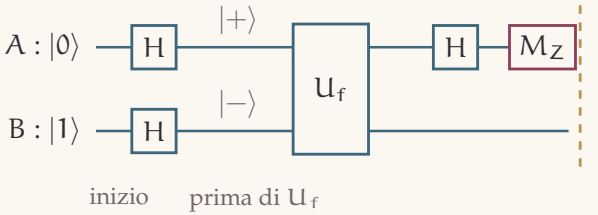
Per una funzione bilanciata i due valori differiscono, dunque $d = f(0) \oplus f(1) = 1$ e $(-1)^d = -1$. Applichiamo le stesse espressioni delle ampiezze: il cambio di segno scambia il contributo che si annulla.

$$c_0 = \frac{1 + (-1)}{2} = 0/2 = 0, \qquad c_1 = \frac{1 - (-1)}{2} = 2/2 = 1.$$

Quindi $H|\phi\rangle = 0|0\rangle + 1|1\rangle = |1\rangle$. La regola di Born fornisce

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

La probabilità totale è $0 + 1 = 1$. La misura restituisce con certezza 1, che coincide con la classificazione cercata. Il fattore globale $(-1)^{f(0)}$ conserva questi pesi.



Stato alla sezione

$$|\psi_3\rangle = (-1)^{f(0)}|1\rangle_A|-\rangle_B$$

La misura legge A nella base computazionale. Il secondo qubit resta nello stesso fattore.

Il circuito determina la classe con un'interrogazione. Il ruolo dello stato meno permette di interpretare il meccanismo che ha prodotto i segni.

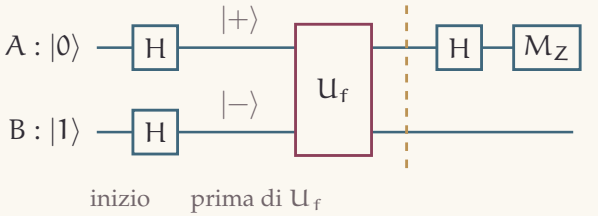
A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $p_A(j) = |c_j|^2$ per $c_0|0\rangle + c_1|1\rangle$ normalizzato; $|z|^2 = z^*z$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Interpretare il ruolo dell'autostato ausiliario

La derivazione ha mostrato che l'ausiliario conserva il fattore $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, mentre i valori della funzione diventano segni. Possiamo ora interpretare questo risultato: quando $f(x) = 1$, l'oracolo applica al bersaglio la porta X. Calcoliamone l'azione:

$$\begin{aligned} X|-\rangle &= \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot(-1) \\ 1\cdot 1 + 0\cdot(-1) \end{pmatrix} \\ &= \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = -|-\rangle. \end{aligned}$$

Un vettore restituito come multiplo di sé è un autovettore; il moltiplicatore è l'autovalore. Qui l'autovalore è -1.



Stato alla sezione

$|\psi_2\rangle = U_f|\psi_1\rangle$

Se $f(x) = 0$, l'oracolo conserva l'ausiliario; se $f(x) = 1$, applica X e produce il segno appena calcolato.

La preparazione in $|-\rangle$ spiega il meccanismo dei segni che abbiamo già ricavato attraverso lo XOR.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $Xv = \lambda v$: autovettore $v \neq 0$, autovalore λ. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

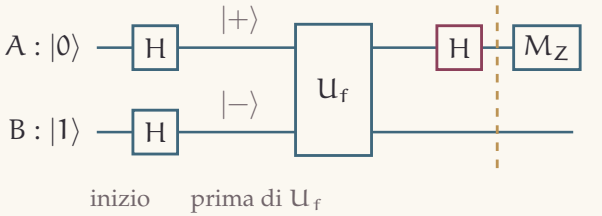
Interpretare gli stati che codificano la risposta

Il ruolo dell'ausiliario è stato chiarito attraverso $X|-\rangle = -|-\rangle$. Il primo registro contiene invece la risposta nei due stati $|+\rangle$ e $|-\rangle$. Verifichiamo anche l'azione di X sullo stato più, così da caratterizzare entrambi i possibili risultati prima della Hadamard:

$$X|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle.$$

Dopo l'oracolo, il primo registro ha il fattore $|\phi\rangle = (|0\rangle + (-1)^d|1\rangle)/\sqrt{2}$. Quindi

d	$\lvert\phi\rangle$	$X\lvert\phi\rangle$
0	$\lvert+\rangle$	$+\lvert+\rangle$
1	$\lvert-\rangle$	$-\lvert-\rangle$



Stato alla sezione

$$|\psi_3\rangle = (-1)^{f(0)}|d\rangle_A|-\rangle_B$$

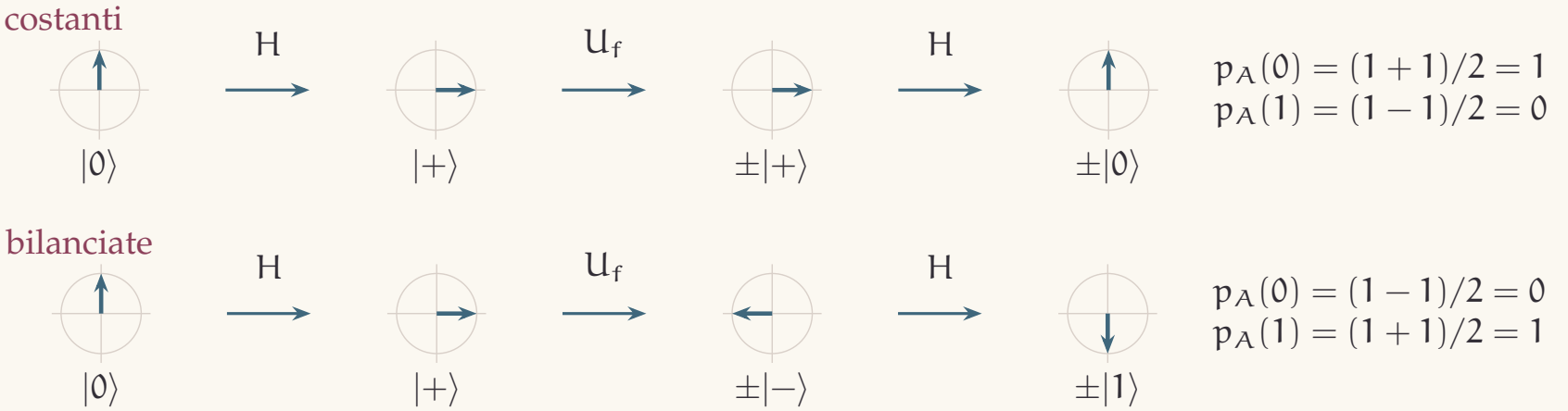
La Hadamard finale li porta a $|0\rangle$ e $|1\rangle$, come mostrano i prodotti già svolti. Il bit misurato è d; l'autovalore di X prima di H è $(-1)^d$.

La risposta si legge trasformando gli stati più e meno in zero e uno. Il diagramma seguente riunisce gli stati attraversati dal primo qubit.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente. Nella misura computazionale, $Z|0\rangle = |0\rangle$ e $Z|1\rangle = -|1\rangle$.

Seguire l'intero percorso geometrico della risposta

Il primo qubit passa da $|0\rangle$ a $|+\rangle$. Con il bersaglio $|-\rangle$, l'oracolo produce le direzioni delle due classi; Hadamard le porta sui poli della misura.



Ai poli usiamo $p_A(0) = (1 + r_z)/2$ e $p_A(1) = (1 - r_z)/2$. I calcoli a destra sviluppano entrambe le probabilità per ciascun polo. Il segno globale conserva il punto; le frecce collegano stati prima e dopo le porte.

Le traiettorie descrivono il caso a un bit. Il confronto dei costi motiva l'estensione a un registro con più qubit.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Assi: r_x orizzontale, r_z verticale; $r_y = 0$. $|0\rangle : (0,1)$, $|+\rangle : (1,0)$, $|-\rangle : (-1,0)$, $|1\rangle : (0,-1)$ nel piano (r_x, r_z). $H|0\rangle = |+\rangle$; $H|+\rangle = |0\rangle$, $H|-\rangle = |1\rangle$. Coordinate: $|0\rangle : (0,0,1)$, $|1\rangle : (0,0,-1)$, $|+\rangle : (1,0,0)$, $|-\rangle : (-1,0,0)$. I calcoli sono nella prima sezione geometrica.

Collegare la risposta al costo delle interrogazioni

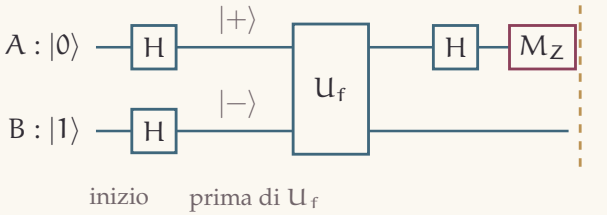
Il calcolo e la rappresentazione geometrica hanno condotto allo stesso stato finale. Riprendiamo la sua espressione per distinguere la risposta ottenuta dalle risorse impiegate per determinarla:

$$|\psi_3\rangle = (-1)^{f(0)}|f(0) \oplus f(1)\rangle \otimes |-\rangle.$$

La misura del primo registro restituisce dunque la classe con certezza. Nell'intera sequenza compare una sola applicazione di U_f; gli altri blocchi sono tre Hadamard e una misura.

procedura esatta	interrogazioni
classica	2
quantistica, accesso coerente	1

Il costo conta gli accessi alla funzione. Estendendo l'ingresso a n bit, le stringhe diventano 2^n. Studiamo la classificazione su questo dominio più ampio.



Stato alla sezione

$$|\psi_3\rangle = (-1)^{f(0)}|d\rangle_A|-\rangle_B$$

Deutsch–Jozsa generalizza la preparazione e l'interferenza, mantenendo un unico qubit ausiliario.

A: primo qubit; B: ausiliario; $|x\rangle|y\rangle = |x\rangle \otimes |y\rangle = |xy\rangle$; base $(00, 01, 10, 11)$. $d = f(0) \oplus f(1)$: $d = 0$ costante, $d = 1$ bilanciata. $U_f|x\rangle|y\rangle = |x\rangle|f(x) \oplus y\rangle$, esteso per linearità. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. M_Z: misura di A in $(|0\rangle, |1\rangle)$; oro: sezione; bordeaux: porta corrente.

Estendere il problema alle stringhe di bit

Il caso a un bit confrontava due valori. Consideriamo ora $f : \{0,1\}^n \to \{0,1\}$: gli ingressi sono 2^n stringhe. Usiamo n per la lunghezza e conserviamo d per il bit di classificazione.

Il problema di Deutsch–Jozsa assume che la funzione sia *costante* oppure *bilanciata*: nel secondo caso produce 2^{n-1} zeri e 2^{n-1} uni. Questa ipotesi è la promessa del problema.

Per $n = 2$, gli ingressi sono $00, 01, 10, 11$. Le tre tabelle mostrano perché la promessa deve essere dichiarata:

x	00	01	10	11	classe
$f(x)$	0	0	0	0	costante
$g(x)$	0	1	1	0	bilanciata
$h(x)$	0	0	0	1	esterna alla promessa

La richiesta resta stabilire la classe, usando il dispositivo che valuta la funzione.

Per misurare il vantaggio della nuova procedura, determiniamo prima quante interrogazioni servano per una risposta classica certa.

n: numero di bit dell'ingresso; $\{0,1\}^n$: tutte le stringhe di lunghezza n. Per $n = 2$, $2^n = 4$ e $2^{n-1} = 2$. Il bit finale d vale 0 per una funzione costante e 1 per una bilanciata.

Quattro risposte uguali lasciano due possibilità

Prendiamo $n = 3$, quindi $2^3 = 8$ ingressi. Interroghiamo quattro stringhe distinte e riceviamo sempre zero. La riga osservata ammette ancora due completamenti compatibili con la promessa:

	000	001	010	011	100	101	110	111
osservato	0	0	0	0	?	?	?	?
costante	0	0	0	0	0	0	0	0
bilanciata	0	0	0	0	1	1	1	1

Nel primo completamento tutti gli otto valori sono zero. Nel secondo, i quattro valori ancora ignoti sono uno: gli zeri e gli uni sono entrambi quattro.
Una quinta interrogazione su un ingresso nuovo decide la classe. Una risposta 1 esclude la funzione costante; una risposta 0 porta a cinque zeri, mentre una funzione bilanciata può averne soltanto quattro.

Il caso con risposte tutte uguali determina il costo nel caso peggiore. Lo stesso conteggio si estende a qualunque lunghezza.

$n = 3$; $N = 2^3 = 8$ ingressi. Una funzione bilanciata ha $N/2 = 4$ zeri e 4 uni. Ogni interrogazione classica sceglie una stringa e restituisce il singolo valore $f(x)$.

Ricavare il costo classico per n bit

Poniamo $N = 2^n$. Dopo $N/2$ interrogazioni distinte con risposta sempre $b \in \{0, 1\}$, restano due funzioni compatibili: la costante b e una bilanciata che vale $1 - b$ sugli ingressi ancora ignoti. Occorre quindi almeno un'altra interrogazione nel caso peggiore. Sono sufficienti $N/2 + 1$ interrogazioni: se compaiono entrambi i valori, la funzione è bilanciata; se tutte le risposte coincidono, la promessa impone che sia costante.

$$Q_{\text{classico,esatto}}(n) = \frac{2^n}{2} + 1 = 2^{n-1} + 1.$$

Per esempio,

$$n = 3: \quad Q = 2^2 + 1 = 4 + 1 = 5, \qquad n = 10: \quad Q = 2^9 + 1 = 512 + 1 = 513.$$

La crescita dipende dal numero di ingressi possibili. Cerchiamo una procedura che ricavi la classe attraverso un'unica applicazione coerente dell'oracolo.

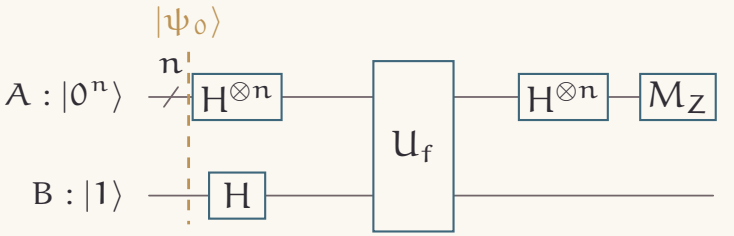
Ampliamo il registro A e manteniamo il medesimo ausiliario B. La struttura del circuito di Deutsch rimane riconoscibile.

Q: numero di interrogazioni alla funzione. Il confronto richiede una classificazione sempre corretta e assume la promessa costante/bilanciata. Gli ingressi delle interrogazioni classiche considerate sono distinti.

Ampliare il registro conservando il circuito

Il registro A contiene n qubit e rappresenta la stringa $x = x_1 \cdots x_n$. B rimane un qubit, perché il valore $f(x)$ è ancora un bit. La regola dell'oracolo diventa

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



A: n qubit; B: un qubit

Prepariamo $|\psi_0\rangle = |0^n\rangle_A|1\rangle_B$. Le sezioni successive sono

$$|\psi_1\rangle = (H^{\otimes n} \otimes H)|\psi_0\rangle, \quad |\psi_2\rangle = U_f|\psi_1\rangle, \quad |\psi_3\rangle = (H^{\otimes n} \otimes I_2)|\psi_2\rangle.$$

Il tratto marcato con n riunisce i fili di A. Seguiamo il caso a due bit.

L'esempio a due bit rende visibili le somme che useremo poi nella derivazione per n bit.

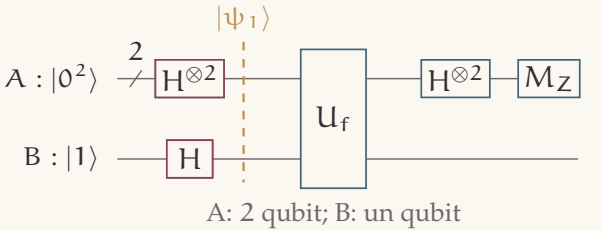
$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $H^{\otimes n}$: una Hadamard su ciascun qubit di A; $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. Oro: sezione dello stato; bordeaux: operazione corrente.

Preparare i due bit dell'esempio

Studiamo $f(x_1, x_2) = x_1 \oplus x_2$, una funzione bilanciata il cui oracolo si costruisce con due CNOT. Per seguirne l'esecuzione partiamo da $|\psi_0\rangle = |00\rangle_A|1\rangle_B$, con $n = 2$. Ogni Hadamard agisce sul proprio fattore. Usando $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ e $H|1\rangle = |-\rangle$, otteniamo

$$\begin{aligned} |\psi_1\rangle &= (H|0\rangle) \otimes (H|0\rangle) \otimes (H|1\rangle) \\ &= \frac{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)}{2} \otimes |-\rangle \\ &= \frac{|00\rangle + |01\rangle + |10\rangle + |11\rangle}{2} \otimes |-\rangle. \end{aligned}$$

Le quattro stringhe di A hanno ampiezza $1/2$ e norma quadrata $4|1/2|^2 = 4/4 = 1$. La norma quadrata di B è $(1^2 + (-1)^2)/2 = 2/2 = 1$. L'ingresso dell'oracolo è dunque normalizzato.



A: 2 qubit; B: un qubit

$$|\psi_1\rangle = |+\rangle|+\rangle|-\rangle.$$

A contiene quattro ampiezze; B prepara i due segni opposti.

La preparazione include tutti gli argomenti con uguale ampiezza e pone B nello stato meno. Definiamo ora l'aggiornamento dell'oracolo e costruiamone le due porte.

A: due qubit, base $(00, 01, 10, 11)$; B: ausiliario. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $|x, y\rangle = |x\rangle_A \otimes |y\rangle_B$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Dallo XOR all'aggiornamento reversibile

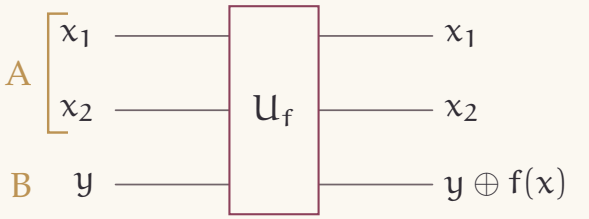
La funzione $f(x_1, x_2) = x_1 \oplus x_2$ permette di costruire un oracolo attraverso due porte già note. La tabella associa un risultato a ciascuna coppia:

x_1x_2	00	01	10	11
$f(x_1, x_2)$	$0 \oplus 0 = 0$	$0 \oplus 1 = 1$	$1 \oplus 0 = 1$	$1 \oplus 1 = 0$

Due zeri e due uni soddisfano la promessa bilanciata. Per conservare gli argomenti, U_f aggiorna un terzo qubit:

$$U_f|x_1, x_2, y\rangle = |x_1, x_2, y \oplus f(x_1, x_2)\rangle.$$

Con $y = 0$, $y \oplus f = 0 \oplus f = f$. Con $y = 1$, $y \oplus f = 1 \oplus f = 1 - f$. L'uscita di B coincide dunque con il valore della funzione quando B parte da zero.



A conserva l'argomento; B riceve l'aggiornamento.

La funzione è assegnata per verificare l'esempio. L'algoritmo di classificazione usa lo stesso circuito esterno quando la funzione rimane ignota.

Realizziamo l'aggiornamento aggiungendo prima il primo bit e poi il secondo, entrambi modulo due.

$A = (x_1, x_2)$; $B = y$. Ordine dei fili e dei fattori: x_1, x_2, y. $f(x) = x_1 \oplus x_2$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. CNOT: $|c, t\rangle \mapsto |c, t \oplus c\rangle$.

Comporre due CNOT sullo stesso bersaglio

Indichiamo con C_1 la CNOT controllata da x_1 e con C_2 quella controllata da x_2. Le porte condividono B, quindi la seconda usa il valore prodotto dalla prima:

$$|x_1, x_2, y\rangle \xrightarrow{C_1} |x_1, x_2, y \oplus x_1\rangle \xrightarrow{C_2} |x_1, x_2, (y \oplus x_1) \oplus x_2\rangle.$$

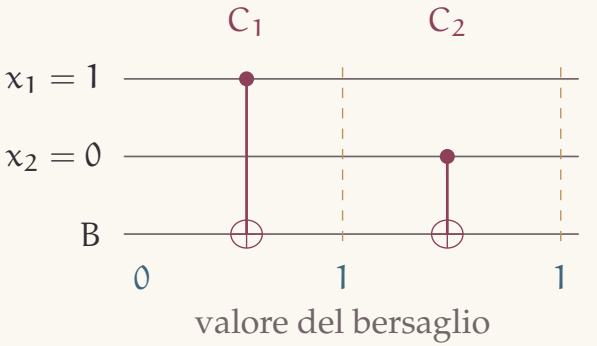
Per associatività, $(y \oplus x_1) \oplus x_2 = y \oplus (x_1 \oplus x_2) = y \oplus f(x)$. Pertanto $U_f = C_2 C_1$.

Prendiamo $x_1 x_2 = 10$ e $y = 0$. La prima porta inverte B; il secondo controllo è zero:

$$|100\rangle \xrightarrow{C_1} |10, 0 \oplus 1\rangle = |101\rangle,$$

$$|101\rangle \xrightarrow{C_2} |10, 1 \oplus 0\rangle = |101\rangle.$$

Il bersaglio finale vale uno, in accordo con $f(1,0) = 1 \oplus 0 = 1$.



Valori di B lungo il circuito:
$0 \to 1 \to 1$.

Il primo esempio attiva una sola inversione. Con entrambi i controlli a uno, seguiremo due inversioni consecutive.

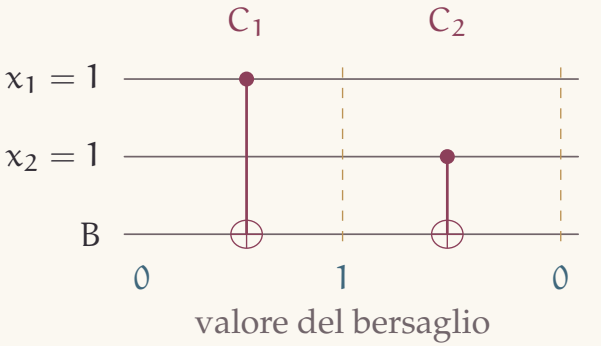
$A = (x_1, x_2)$; $B = y$. Ordine dei fili e dei fattori: x_1, x_2, y. $f(x) = x_1 \oplus x_2$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. CNOT: $|c, t\rangle \mapsto |c, t \oplus c\rangle$.

Due inversioni restituiscono il valore iniziale

Manteniamo $y = 0$ e scegliamo $x_1 x_2 = 11$ per attivare entrambe le CNOT. Il circuito è lo stesso; cambiano i valori dei controlli:

$$|110\rangle \xrightarrow{C_1} |11, 0 \oplus 1\rangle = |111\rangle,$$
$$|111\rangle \xrightarrow{C_2} |11, 1 \oplus 1\rangle = |110\rangle.$$

La prima inversione porta B da zero a uno; la seconda lo riporta a zero. Otteniamo $f(1,1) = 1 \oplus 1 = 0$.
Lo XOR registra la parità delle inversioni: una produce uno, due restituiscono zero. AND, invece, vale $1 \cdot 1 = 1$ su questa stessa coppia; Toffoli applicherebbe una sola inversione del bersaglio.



Valori di B: $0 \to 1 \to 0$.

L'esempio distingue così la composizione di due CNOT dalla porta con due controlli. Completiamo la verifica includendo anche un ausiliario iniziale uguale a uno.

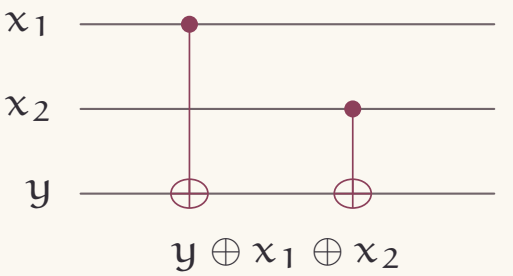
La scelta del bersaglio iniziale determina come interpretarne l'uscita. La tabella seguente esplicita tutti gli ingressi della base.

$A = (x_1, x_2)$; $B = y$. Ordine dei fili e dei fattori: x_1, x_2, y. $f(x) = x_1 \oplus x_2$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. CNOT: $|c, t\rangle \mapsto |c, t \oplus c\rangle$.

Verificare gli otto ingressi dell'oracolo

Per $f = x_1 \oplus x_2$, poniamo $u = y \oplus x_1$ e $v = u \oplus x_2$. Ogni riga confronta le due CNOT con $v = y \oplus f(x)$:

x_1x_2y	$u = y \oplus x_1$	dopo C_1	$v = u \oplus x_2$	dopo C_2	$y \oplus f(x)$
000	$0 \oplus 0 = 0$	$\lvert 000\rangle$	$0 \oplus 0 = 0$	$\lvert 000\rangle$	$0 \oplus 0 = 0$
001	$1 \oplus 0 = 1$	$\lvert 001\rangle$	$1 \oplus 0 = 1$	$\lvert 001\rangle$	$1 \oplus 0 = 1$
010	$0 \oplus 0 = 0$	$\lvert 010\rangle$	$0 \oplus 1 = 1$	$\lvert 011\rangle$	$0 \oplus 1 = 1$
011	$1 \oplus 0 = 1$	$\lvert 011\rangle$	$1 \oplus 1 = 0$	$\lvert 010\rangle$	$1 \oplus 1 = 0$
100	$0 \oplus 1 = 1$	$\lvert 101\rangle$	$1 \oplus 0 = 1$	$\lvert 101\rangle$	$0 \oplus 1 = 1$
101	$1 \oplus 1 = 0$	$\lvert 100\rangle$	$0 \oplus 0 = 0$	$\lvert 100\rangle$	$1 \oplus 1 = 0$
110	$0 \oplus 1 = 1$	$\lvert 111\rangle$	$1 \oplus 1 = 0$	$\lvert 110\rangle$	$0 \oplus 0 = 0$
111	$1 \oplus 1 = 0$	$\lvert 110\rangle$	$0 \oplus 1 = 1$	$\lvert 111\rangle$	$1 \oplus 0 = 1$



Le otto uscite sono distinte. I controlli restano disponibili e permettono di invertire l'aggiornamento.

La tabella definisce l'azione sulla base. Per linearità, la stessa porta agisce sulle sovrapposizioni.

Le due CNOT sono le porte interne di una chiamata a U_f. Passiamo dall'aggiornamento dei bit ai segni delle ampiezze.

$A = (x_1, x_2)$; $B = y$. Ordine dei fili e dei fattori: x_1, x_2, y. $f(x) = x_1 \oplus x_2$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. CNOT: $|c, t\rangle \mapsto |c, t \oplus c\rangle$.

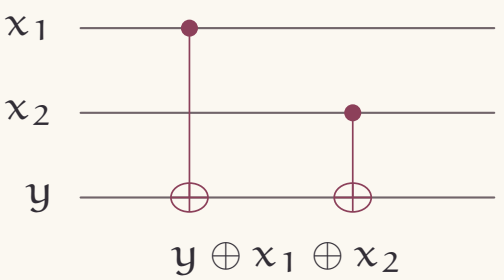
Lo stato meno trasforma gli scambi in segni

L'algoritmo prepara B in $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$, perché X restituisce questo vettore con segno opposto. Seguiamo le due CNOT per ciascun argomento:

La prima applica X se $x_1 = 1$; la seconda se $x_2 = 1$. L'identità conserva $|-\rangle$: $I_2|-\rangle = |-\rangle$.

$$
\begin{aligned}
|00\rangle|-\rangle &\xrightarrow{C_1} |00\rangle|-\rangle \xrightarrow{C_2} |00\rangle|-\rangle,\\
|01\rangle|-\rangle &\xrightarrow{C_1} |01\rangle|-\rangle \xrightarrow{C_2} -|01\rangle|-\rangle,\\
|10\rangle|-\rangle &\xrightarrow{C_1} -|10\rangle|-\rangle \xrightarrow{C_2} -|10\rangle|-\rangle,\\
|11\rangle|-\rangle &\xrightarrow{C_1} -|11\rangle|-\rangle \xrightarrow{C_2} (-1)(-1)|11\rangle|-\rangle\\
&\qquad = |11\rangle|-\rangle.
\end{aligned}
$$

I segni sono $+, -, -, +$, cioè $(-1)^{f(x)}$. Nella sovrapposizione degli argomenti sono relativi e intervengono nella ricombinazione.



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

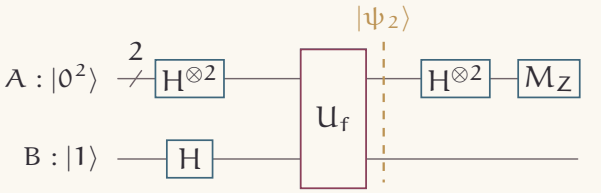
Le quattro righe sviluppano una sola applicazione lineare dell'oracolo. Ricomponiamo i contributi con il coefficiente iniziale $1/2$.

$A = (x_1, x_2)$; $B = y$. Ordine dei fili e dei fattori: x_1, x_2, y. $f(x) = x_1 \oplus x_2$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. CNOT: $|c, t\rangle \mapsto |c, t \oplus c\rangle$. $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$; $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Ricomporre i segni prodotti dall'oracolo

La preparazione ha dato $|\psi_1\rangle = (|00\rangle + |01\rangle + |10\rangle + |11\rangle)|-\rangle/2$. Le immagini ottenute sono $|00\rangle|-\rangle$, $-|01\rangle|-\rangle$, $-|10\rangle|-\rangle$ e $|11\rangle|-\rangle$. La linearità conserva il coefficiente $1/2$ di ogni contributo:

$$\begin{aligned}|\psi_2\rangle &= \frac{1}{2}\big[|00\rangle|-\rangle - |01\rangle|-\rangle \\ &\qquad - |10\rangle|-\rangle + |11\rangle|-\rangle\big] \\ &= \underbrace{\frac{|00\rangle - |01\rangle - |10\rangle + |11\rangle}{2}}_{|\chi\rangle_A} \otimes |-\rangle_B .\end{aligned}$$



A: 2 qubit; B: un qubit



ampiezze: coefficiente $\times 1/2$

Nella base $(00, 01, 10, 11)$, il vettore è $|\chi\rangle = (1, -1, -1, 1)^T/2$. Le probabilità prima dell'ultima trasformazione sono tutte $|\pm 1/2|^2 = 1/4$. L'informazione sulla funzione è nei segni che Hadamard deve combinare.

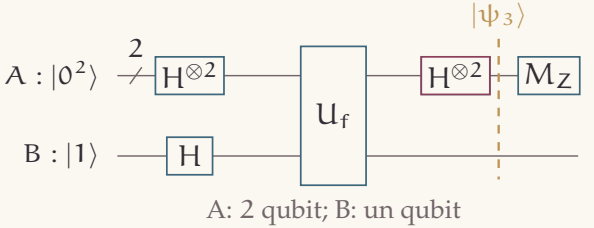
Applichiamo H a entrambi i qubit di A. Ogni riga della matrice determina una diversa combinazione dei quattro segni.

A: due qubit, base $(00, 01, 10, 11)$; B: ausiliario. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $|x, y\rangle = |x\rangle_A \otimes |y\rangle_B$. $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Calcolare le quattro ampiezze dopo Hadamard

Ripartiamo da $|\chi\rangle = (1,-1,-1,1)^{\mathsf{T}}/2$. La matrice della porta finale su A è

$$H^{\otimes 2} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$



A: 2 qubit; B: un qubit

Il fattore comune del prodotto è $(1/2)(1/2) = 1/4$. Calcoliamo ogni numeratore:

$$4\alpha_{00} = 1\cdot 1 + 1(-1) + 1(-1) + 1\cdot 1 = 1 - 1 - 1 + 1 = 0,$$
$$4\alpha_{01} = 1\cdot 1 + (-1)(-1) + 1(-1) + (-1)1 = 1 + 1 - 1 - 1 = 0,$$
$$4\alpha_{10} = 1\cdot 1 + 1(-1) + (-1)(-1) + (-1)1 = 1 - 1 + 1 - 1 = 0,$$
$$4\alpha_{11} = 1\cdot 1 + (-1)(-1) + (-1)(-1) + 1\cdot 1 = 1 + 1 + 1 + 1 = 4.$$

Quindi $H^{\otimes 2}|\chi\rangle = (0/4, 0/4, 0/4, 4/4)^{\mathsf{T}} = |11\rangle$.

La ricombinazione annulla tre ampiezze e conserva soltanto quella della stringa 11. Interpretiamo la misura del registro.

A: due qubit, base $(00,01,10,11)$; B: ausiliario. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $|x,y\rangle = |x\rangle_A \otimes |y\rangle_B$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Leggere la classe nella stringa misurata

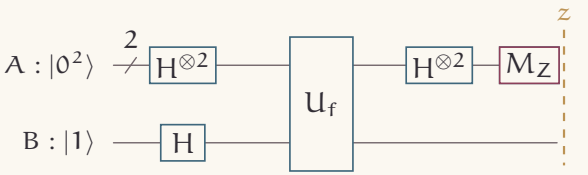
La trasformazione ha prodotto $|\psi_3\rangle = |11\rangle_A|-\rangle_B$. Le ampiezze di A sono $(0,0,0,1)^T$, quindi Born dà

$$p(00) = |0|^2 = 0, \quad p(01) = |0|^2 = 0,$$
$$p(10) = |0|^2 = 0, \quad p(11) = |1|^2 = 1.$$

La somma è $0+0+0+1=1$. A restituisce $z = 11$ con certezza. La regola di decisione assegna $d = 1$ quando almeno un bit misurato vale uno:

$$d = z_1 \vee z_2 = 1 \vee 1 = 1.$$

Otteniamo dunque la classe bilanciata, coerentemente con la tabella $(0,1,1,0)$ dell'esempio. Il simbolo $\vee$ indica OR: vale zero soltanto quando entrambi i bit sono zero.
Estendiamo il risultato a una funzione ammessa qualunque, usando somme sulle stringhe.



A: 2 qubit; B: un qubit

z: stringa osservata.
d: classe della funzione.

B rimane nello stato $|-\rangle$.

La derivazione generale deve spiegare perché l'esito tutto zero distingua le due classi, anche quando gli altri esiti hanno probabilità diverse.

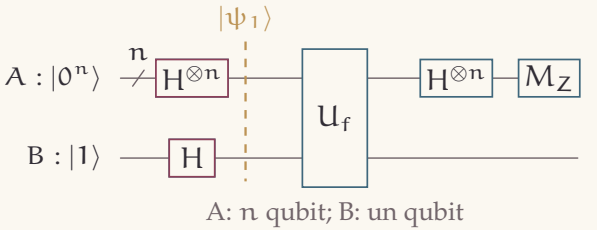
A: due qubit, base $(00,01,10,11)$; B: ausiliario. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $|x,y\rangle = |x\rangle_A \otimes |y\rangle_B$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$; $I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Scrivere la preparazione per n qubit

Riprendiamo $|\psi_0\rangle = |0^n\rangle_A|1\rangle_B$. Su ogni qubit di A, $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Distribuendo il prodotto dei n fattori, ciascuna scelta $x_1, \ldots, x_n$ genera una stringa:

$$\begin{aligned} H^{\otimes n}|0^n\rangle &= \bigotimes_{j=1}^{n} \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ &= \frac{1}{(\sqrt{2})^n} \sum_{x_1=0}^{1} \cdots \sum_{x_n=0}^{1} |x_1 \cdots x_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle. \end{aligned}$$

La norma quadrata è $2^n \cdot |1/\sqrt{2^n}|^2 = 2^n/2^n = 1$, perché tutti i 2^n coefficienti hanno lo stesso modulo.



A: n qubit; B: un qubit

Per B, $H|1\rangle = |-\rangle$. Lo stato complessivo è

$$|\psi_1\rangle = \left[\frac{1}{\sqrt{2^n}} \sum_x |x\rangle_A\right] \otimes |-\rangle_B.$$

Ogni stringa ha lo stesso peso iniziale. L'oracolo sostituisce questa uniformità dei segni con quella determinata dai valori della funzione.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $(\sqrt{2})^n = \sqrt{2^n}$.

Applicare la stessa regola di fase a ogni stringa

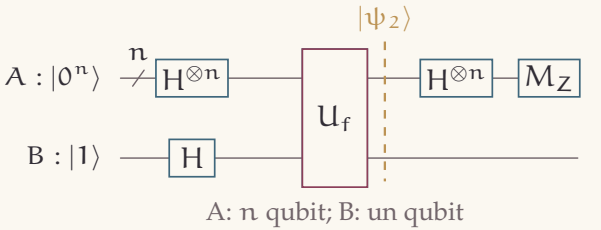
L'ingresso è $|\psi_1\rangle = 2^{-n/2}\sum_x |x\rangle|-\rangle$. L'identità già usata in Deutsch vale per ogni stringa, perché $f(x)$ rimane un singolo bit:

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

Usiamo la linearità e raccogliamo il fattore comune dell'ausiliario:

$$\begin{aligned}|\psi_2\rangle &= U_f\left(\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|-\rangle\right)\\ &= \frac{1}{\sqrt{2^n}}\sum_x U_f|x\rangle|-\rangle\\ &= \frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle|-\rangle.\end{aligned}$$

Il segno è positivo dove $f(x) = 0$ e negativo dove $f(x) = 1$. La fase dell'ausiliario permette così di rappresentare la funzione nei coefficienti di A.



A: n qubit; B: un qubit

Raccogliamo il fattore comune di B:

$$|\psi_2\rangle = \left[\frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle\right] \otimes |-\rangle.$$

Per ricombinare questi coefficienti dobbiamo descrivere come H su tutti i qubit colleghi ogni ingresso x a ciascun esito z.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $X|-\rangle = -|-\rangle$; $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. $(-1)^0 = 1$, $(-1)^1 = -1$.

Associare un segno a ogni coppia di stringhe

Nel caso a due bit, ogni riga di $H^{\otimes 2}$ combina le quattro ampiezze con segni precisi. Indichiamo con x la colonna dell'ingresso e con z la riga dell'uscita.
Definiamo il prodotto binario

$$x \cdot z = x_1 z_1 \oplus \cdots \oplus x_n z_n.$$

Ogni prodotto $x_j z_j$ vale 0 oppure 1; lo XOR finale restituisce la parità del numero di prodotti uguali a uno. Per esempio,

$$x = 10,\ z = 11: \quad x \cdot z = 1 \cdot 1 \oplus 0 \cdot 1 = 1 \oplus 0 = 1,$$
$$(-1)^{x \cdot z} = (-1)^1 = -1;$$
$$x = 11,\ z = 11: \quad x \cdot z = 1 \cdot 1 \oplus 1 \cdot 1 = 1 \oplus 1 = 0,$$
$$(-1)^{x \cdot z} = (-1)^0 = 1.$$

I due risultati coincidono con le celle della riga 11. Deriviamo ora questa regola dal prodotto delle Hadamard.

$z \backslash x$	00	01	10	11
00	+1	+1	+1	+1
01	+1	−1	+1	−1
10	+1	+1	−1	−1
11	+1	−1	−1	+1

segni di $\langle z|H^{\otimes 2}|x\rangle$

Per $n = 2$, ogni elemento della matrice è il segno indicato diviso per $\sqrt{2^2} = 2$.

La notazione descrive i segni del prodotto matriciale già eseguito. L'espansione successiva ne stabilisce la validità per qualsiasi n.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $x \cdot z$ è un bit; equivale a $(\sum_j x_j z_j) \bmod 2$.

Espandere la Hadamard sull'intero registro

Per un bit x_j, le due immagini note si scrivono insieme:

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

Nel prodotto, gli indici $z_1, \ldots, z_n$ formano la stringa z:

$$\begin{aligned} H^{\otimes n}|x\rangle &= \bigotimes_{j=1}^{n} H|x_j\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{z_1=0}^{1} \cdots \sum_{z_n=0}^{1} \left[\prod_{j=1}^{n} (-1)^{x_j z_j}\right] |z_1 \cdots z_n\rangle \\ &= \frac{1}{\sqrt{2^n}} \sum_{z} (-1)^{\sum_j x_j z_j} |z\rangle = \frac{1}{\sqrt{2^n}} \sum_{z} (-1)^{x\cdot z} |z\rangle. \end{aligned}$$

Sommando gli esponenti conta soltanto la parità: $(-1)^{2m} = 1$ e $(-1)^{2m+1} = -1$.

Sostituiamo questa espressione nello stato prodotto dall'oracolo, mantenendo esplicito il contributo di ogni ingresso.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$; $x \cdot z = (\sum_j x_j z_j) \bmod 2$. $\prod_j$ indica il prodotto dei fattori.

Raccogliere i contributi diretti allo stesso esito

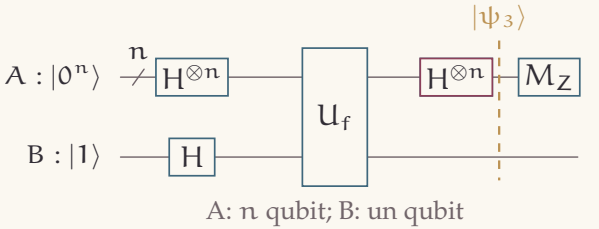
L'oracolo ha dato $|\psi_2\rangle = 2^{-n/2}\sum_x (-1)^{f(x)}|x\rangle|-\rangle$. Applichiamo $H^{\otimes n}$ ad A e sostituiamo l'immagine di ciascun $|x\rangle$:

$$\begin{aligned}|\psi_3\rangle &= \frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)} H^{\otimes n}|x\rangle|-\rangle \\ &= \frac{1}{2^n}\sum_x\sum_z (-1)^{f(x)}(-1)^{x\cdot z}|z\rangle|-\rangle \\ &= \sum_z \left[\frac{1}{2^n}\sum_x (-1)^{f(x)+x\cdot z}\right]|z\rangle|-\rangle.\end{aligned}$$

Le somme sono finite: possiamo raggruppare tutti i termini che accompagnano lo stesso $|z\rangle$. La sua ampiezza è quindi

$$\alpha_z = \frac{1}{2^n}\sum_x (-1)^{f(x)+x\cdot z}.$$

Born darà $p(z) = |\alpha_z|^2$ dopo questa somma.



A: n qubit; B: un qubit

Il prodotto dei coefficienti dà

$$\frac{1}{\sqrt{2^n}}\frac{1}{\sqrt{2^n}} = \frac{1}{2^n}.$$

Ogni ingresso x contribuisce a ogni esito z con il segno indicato dalla Hadamard.

La classificazione dipende dall'esito formato da soli zeri. Per quella riga della trasformazione, tutti i segni di Hadamard sono positivi.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $H^{\otimes n}|x\rangle = 2^{-n/2}\sum_z (-1)^{x\cdot z}|z\rangle$; $x \cdot z = (\sum_j x_j z_j) \bmod 2$.

L'esito tutto zero somma i segni della funzione

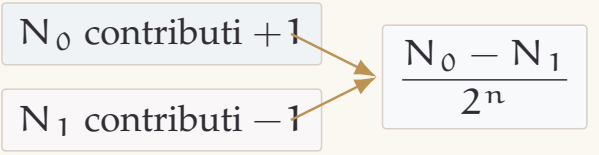
Abbiamo ottenuto $\alpha_z = 2^{-n}\sum_x (-1)^{f(x)+x\cdot z}$. Per $z = 0^n$, ogni prodotto $x_j \cdot 0$ vale zero, dunque $x \cdot 0^n = 0$ e

$$\alpha_{0^n} = \frac{1}{2^n}\sum_x (-1)^{f(x)}.$$

Indichiamo con N_0 il numero di ingressi per cui $f(x) = 0$ e con N_1 quello per cui $f(x) = 1$. Poiché ciascun ingresso appartiene a uno dei due gruppi, $N_0 + N_1 = 2^n$. Separando i contributi,

$$\alpha_{0^n} = \frac{1}{2^n}\left[\sum_{f(x)=0} 1 + \sum_{f(x)=1} (-1)\right] = \frac{N_0 \cdot 1 + N_1 \cdot (-1)}{2^n} = \frac{N_0 - N_1}{2^n}.$$

L'ampiezza misura quindi lo squilibrio fra i due gruppi di valori.



ampiezza dell'esito 0^n

Ogni freccia raccoglie contributi alla stessa ampiezza. La probabilità si ottiene prendendo il modulo quadro della somma.

La promessa impone soltanto due tipi di conteggio. Sostituendoli nella formula ricaviamo gli esiti certi delle due classi.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. N_b: numero di stringhe x con $f(x) = b$; $N_0 + N_1 = 2^n$.

Le funzioni costanti producono la stringa zero

Usiamo $\alpha_{0^n} = (N_0 - N_1)/2^n$. Se $f(x) = 0$ per ogni ingresso, $N_0 = 2^n$ e $N_1 = 0$:

$$\alpha_{0^n} = \frac{2^n - 0}{2^n} = 1, \qquad p(0^n) = |1|^2 = 1.$$

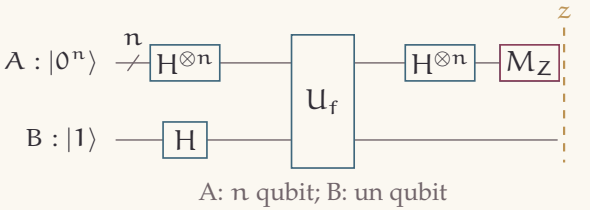
Se $f(x) = 1$ per ogni ingresso, $N_0 = 0$ e $N_1 = 2^n$:

$$\alpha_{0^n} = \frac{0 - 2^n}{2^n} = -1, \qquad p(0^n) = |-1|^2 = 1.$$

La normalizzazione dello stato finale impone

$$\sum_{z \neq 0^n} |\alpha_z|^2 = 1 - |\alpha_{0^n}|^2 = 1 - 1 = 0.$$

Ogni termine della somma è non negativo, quindi ciascuna delle altre probabilità vale zero. La misura restituisce 0^n con certezza e assegniamo $d = 0$.



A: n qubit; B: un qubit

$$p(0^n) = 1.$$

Per $n = 2$, l'esito è 00; per $n = 3$, è 000.

Le due costanti possono differire per il segno globale dello stato. Entrambe concentrano la probabilità nella stringa tutto zero.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $N_b = \#\{x : f(x) = b\}$; $\alpha_{0^n} = (N_0 - N_1)/2^n$. $d = 0$: classe costante.

Le funzioni bilanciate escludono la stringa zero

Per una funzione bilanciata, $N_0 = N_1 = 2^{n-1}$. La stessa formula dà

$$\alpha_{0^n} = \frac{2^{n-1} - 2^{n-1}}{2^n} = \frac{0}{2^n} = 0, \qquad p(0^n) = |0|^2 = 0.$$

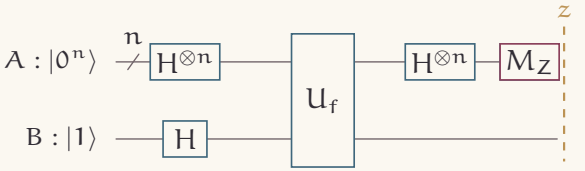
La probabilità complessiva degli altri esiti è

$$\sum_{z \neq 0^n} p(z) = 1 - p(0^n) = 1 - 0 = 1.$$

La misura produce quindi una stringa con almeno un bit uguale a uno. La decisione è

$$d = z_1 \vee z_2 \vee \cdots \vee z_n = 1.$$

Le probabilità delle singole stringhe possono dipendere da f. La certezza riguarda la classe, perché ogni esito possibile esclude 0^n. Per $n = 1$ ritroviamo Deutsch: l'unico esito diverso da zero è 1. Con più bit, una funzione bilanciata può distribuire la probabilità su più esiti.



A: n qubit; B: un qubit

Costruiamo un esempio a tre bit che impiega Toffoli e produce quattro stringhe finali possibili.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. $N_0 = N_1 = 2^{n-1}$; $p(z) = |\alpha_z|^2$. $\vee$: OR dei bit misurati; $d = 1$: classe bilanciata.

Costruire una funzione bilanciata con Toffoli

Lo XOR a due bit ha prodotto un solo esito. Per studiare una classificazione certa con più esiti possibili, scegliamo $n = 3$ e $f(x_1, x_2, x_3) = x_1 \oplus (x_2 x_3)$. Il termine AND permette di usare Toffoli.

x	$x_2 x_3$	$f(x)$
000	$0 \cdot 0 = 0$	$0 \oplus 0 = 0$
001	$0 \cdot 1 = 0$	$0 \oplus 0 = 0$
010	$1 \cdot 0 = 0$	$0 \oplus 0 = 0$
011	$1 \cdot 1 = 1$	$0 \oplus 1 = 1$
100	$0 \cdot 0 = 0$	$1 \oplus 0 = 1$
101	$0 \cdot 1 = 0$	$1 \oplus 0 = 1$
110	$1 \cdot 0 = 0$	$1 \oplus 0 = 1$
111	$1 \cdot 1 = 1$	$1 \oplus 1 = 0$

Fissati x_2, x_3, poniamo $h = x_2 x_3$. Per $x_1 = 0$ si ha $f = 0 \oplus h = h$; per $x_1 = 1$ si ha $f = 1 \oplus h = 1 - h$.

Per $h = 0$ otteniamo $0, 1$; per $h = 1, 1, 0$. Ciascuna delle quattro coppie $x_2 x_3$ produce quindi uno zero e un uno.

La funzione è bilanciata: ci sono quattro zeri e quattro uni. La tabella sviluppa ogni prodotto AND e il successivo XOR.

La promessa è verificata. Costruiamo l'oracolo e seguiamo la distribuzione dei possibili esiti.

A: tre qubit, base $(000, 001, 010, 011, 100, 101, 110, 111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2 x_3)$; $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Seguire i due controlli nell'oracolo composto

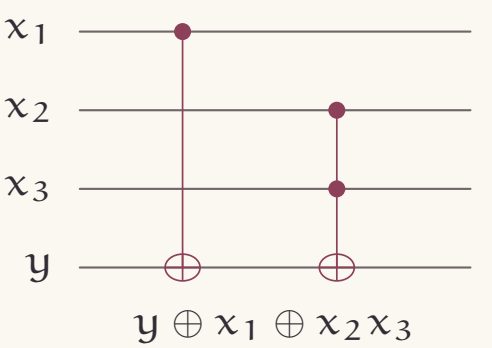
Per $f = x_1 \oplus x_2x_3$, usiamo CNOT da x_1 a B, poi Toffoli da x_2, x_3 a B: $(y \oplus x_1) \oplus (x_2x_3) = y \oplus f(x)$. Con $y = 0$, scegliamo 011 e 111 per confrontare una e due inversioni. Per $x = 011$, la CNOT ha controllo zero; Toffoli ha entrambi i controlli uguali a uno:

$$|011, 0\rangle \xrightarrow{\text{CNOT}} |011, 0 \oplus 0\rangle = |011, 0\rangle$$
$$\xrightarrow{\text{Toffoli}} |011, 0 \oplus (1 \cdot 1)\rangle = |011, 1\rangle.$$

Per $x = 111$, entrambe le porte invertono B:

$$|111, 0\rangle \xrightarrow{\text{CNOT}} |111, 0 \oplus 1\rangle = |111, 1\rangle$$
$$\xrightarrow{\text{Toffoli}} |111, 1 \oplus (1 \cdot 1)\rangle = |111, 0\rangle.$$

Otteniamo rispettivamente $f(011) = 0 \oplus 1 = 1$ e $f(111) = 1 \oplus 1 = 0$. L'effetto della composizione dipende dai tre bit di A.



Nel circuito di classificazione B sarà preparato in meno. Gli stessi scambi assegneranno i segni alle otto componenti.

A: tre qubit, base $(000, 001, 010, 011, 100, 101, 110, 111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2x_3)$; $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Distribuire i segni sulle otto componenti

Con $n = 3$, la preparazione fornisce

$$|\psi_1\rangle = \frac{|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle}{\sqrt{8}} \otimes |-\rangle.$$

La tabella di $f = x_1 \oplus x_2 x_3$ dà i valori $(0,0,0,1,1,1,1,0)$. La regola $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$ assegna dunque i segni $(+,+,+,-,-,-,-,+)$:

$$|\psi_2\rangle = \frac{1}{\sqrt{8}}\big(|000\rangle + |001\rangle + |010\rangle - |011\rangle - |100\rangle - |101\rangle - |110\rangle + |111\rangle\big) \otimes |-\rangle.$$

Ogni peso di A resta $|1/\sqrt{8}|^2 = 1/8$, e la somma è $8/8 = 1$. Per calcolare la Hadamard finale, raggruppiamo i termini secondo il primo bit.

I quattro termini con primo bit uno hanno coefficienti opposti ai corrispondenti termini con primo bit zero. Questo permette una fattorizzazione utile al calcolo.

A: tre qubit, base $(000, 001, 010, 011, 100, 101, 110, 111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2 x_3)$; $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.

Fattorizzare il primo qubit e trasformarlo

Nello stato dopo l'oracolo, poniamo $G = |00\rangle + |01\rangle + |10\rangle - |11\rangle$. Il fattore di A si raccoglie come

$$|\chi\rangle_A = \frac{|0\rangle G - |1\rangle G}{\sqrt{8}} = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \otimes \frac{G}{2} = |-\rangle \otimes |g\rangle,$$

$$|g\rangle = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2}.$$

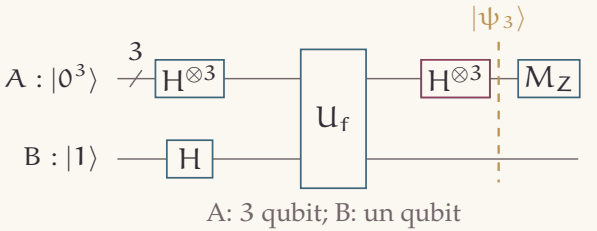
Abbiamo usato $\sqrt{8} = 2\sqrt{2}$. La norma quadrata di $|g\rangle$ è $(1+1+1+1)/4 = 1$. La porta finale separa le azioni sui fattori:

$$H^{\otimes 3}(|-\rangle \otimes |g\rangle) = (H|-\rangle) \otimes (H^{\otimes 2}|g\rangle).$$

Il primo prodotto dà

$$H|-\rangle = \frac{1}{2}\begin{pmatrix} 1\cdot 1 + 1(-1) \\ 1\cdot 1 + (-1)(-1) \end{pmatrix} = \begin{pmatrix} 0/2 \\ 2/2 \end{pmatrix} = |1\rangle.$$

Resta da calcolare l'azione sui due qubit inferiori di A.



A: 3 qubit; B: un qubit

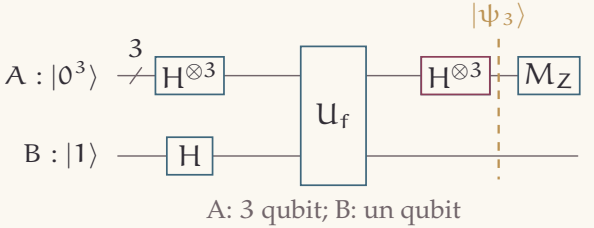
Il primo qubit è uno con certezza. I due rimanenti determineranno i pesi delle stringhe che iniziano con uno.

A: tre qubit, base $(000, 001, 010, 011, 100, 101, 110, 111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2 x_3)$; $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$. $|\psi_2\rangle = |\chi\rangle_A|-\rangle_B$; G è il vettore a due qubit scritto nel corpo; $|g\rangle = G/2$.

Calcolare le quattro ampiezze dei qubit rimanenti

Il fattore da trasformare è $|g\rangle = (1,1,1,-1)^T/2$, nella base $(00,01,10,11)$. Usiamo

$$H^{\otimes 2} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$



A: 3 qubit; B: un qubit

Il fattore comune del prodotto è $1/4$. I quattro numeratori sono

$$4\beta_{00} = 1\cdot 1 + 1\cdot 1 + 1\cdot 1 + 1(-1) = 1+1+1-1 = 2,$$
$$4\beta_{01} = 1\cdot 1 + (-1)1 + 1\cdot 1 + (-1)(-1) = 1-1+1+1 = 2,$$
$$4\beta_{10} = 1\cdot 1 + 1\cdot 1 + (-1)1 + (-1)(-1) = 1+1-1+1 = 2,$$
$$4\beta_{11} = 1\cdot 1 + (-1)1 + (-1)1 + 1(-1) = 1-1-1-1 = -2.$$

Quindi $H^{\otimes 2}|g\rangle = (2,2,2,-2)^T/4 = (1,1,1,-1)^T/2 = |g\rangle$. Il fattore resta invariato.

Il primo qubit di A è diventato uno; gli altri due conservano il vettore g. Ricomponiamo lo stato per calcolare gli esiti della misura.

A: tre qubit, base $(000,001,010,011,100,101,110,111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2 x_3)$; $U_f|x,y\rangle = |x, y\oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$. β_{uv}: ampiezza della coppia degli ultimi due qubit di A.

Classificare con quattro esiti possibili

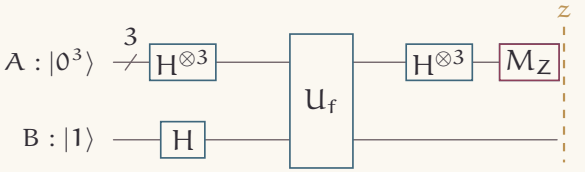
I prodotti hanno dato $H|-\rangle = |1\rangle$ e $H^{\otimes 2}|g\rangle = |g\rangle$, quindi

$$|\psi_3\rangle = |1\rangle \otimes \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2} \otimes |-\rangle$$
$$= \frac{|100\rangle + |101\rangle + |110\rangle - |111\rangle}{2} \otimes |-\rangle.$$

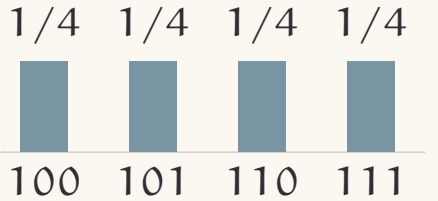
Born fornisce

$$p(100) = p(101) = p(110) = |1/2|^2 = 1/4,$$
$$p(111) = |-1/2|^2 = 1/4.$$

Le altre ampiezze sono nulle, perciò le altre probabilità valgono $|0|^2 = 0$. La somma è $4(1/4) = 1$. Ogni esito possibile inizia con uno: $d = z_1 \vee z_2 \vee z_3 = 1$ in tutti i casi.
Tutti i quattro esiti determinano con certezza la classe bilanciata.



A: 3 qubit; B: un qubit



gli altri quattro esiti hanno probabilità zero

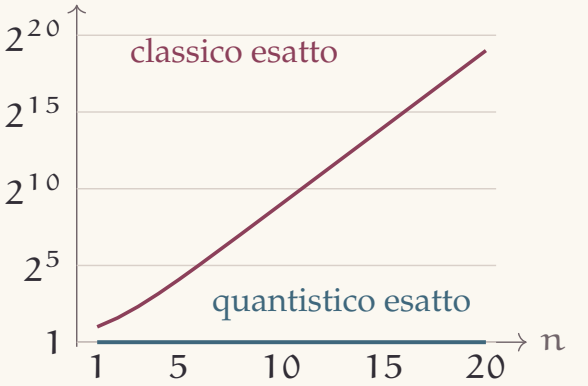
Ogni stringa possibile identifica la stessa classe bilanciata. La preparazione e la lettura ricavano questa proprietà comune, anche quando il singolo esito varia fra esecuzioni.

A: tre qubit, base $(000, 001, 010, 011, 100, 101, 110, 111)$; B: ausiliario. $f(x) = x_1 \oplus (x_2 x_3)$; $U_f|x, y\rangle = |x, y \oplus f(x)\rangle$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p(z) = |\alpha_z|^2$.
$\vee$: OR dei bit; $d = 1$: funzione bilanciata.

Confrontare il numero di interrogazioni esatte

Una chiamata a U_f è sufficiente per ogni n. La procedura classica esatta può richiedere $2^{n-1}+1$ accessi:

n	Q_{classico}	$Q_{\text{quantistico}}$
1	$2^0+1=2$	1
3	$2^2+1=5$	1
10	$2^9+1=513$	1
20	$2^{19}+1=524\,289$	1



La separazione è esponenziale rispetto al numero di interrogazioni necessarie per una risposta sempre corretta.
Il circuito esterno contiene inoltre n Hadamard su A e una su B nella preparazione, poi altre n su A: in totale $n+1+n=2n+1$. Si misurano gli n qubit di A. Il costo delle porte che realizzano U_f dipende dalla funzione ed è distinto dal conteggio degli accessi.

La garanzia di correttezza fa parte del confronto. Se si ammette una probabilità di errore, il costo del campionamento classico cambia.

$n \geq 1$ intero. A: registro di n qubit; B: un qubit ausiliario. $x = x_1 \cdots x_n \in \{0,1\}^n$, base lessicografica; $\sum_x$ percorre tutte le 2^n stringhe. $|0^n\rangle = |0\rangle^{\otimes n}$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$; $\oplus$: somma modulo due. Q: applicazioni dell'oracolo. La scala verticale del grafico è logaritmica; intervalli verticali uguali corrispondono allo stesso fattore moltiplicativo. Le tacche consecutive moltiplicano il costo per $2^5 = 32$.

Precisare il confronto quando si ammettono errori

Consideriamo k ingressi estratti uniformemente e indipendentemente, ammettendo ripetizioni. Una procedura classica dichiara la classe costante se tutte le risposte coincidono; altrimenti dichiara la classe bilanciata.

Per una funzione costante la risposta è sempre corretta. Per una bilanciata, ciascuna estrazione dà 0 oppure 1 con probabilità $1/2$. L'errore si verifica nei due eventi disgiunti «tutti zero» e «tutti uno»:

$$\mathrm{P}(\text{errore} \mid f \text{ bilanciata}) = \left(\frac{1}{2}\right)^{k} + \left(\frac{1}{2}\right)^{k} = \frac{2}{2^{k}} = 2^{1-k}.$$

Per $k = 11$, $\mathrm{P}(\text{errore}) = 2^{-10} = 1/1024 < 1/1000$: la probabilità di successo supera il 99,9%, indipendentemente da n.

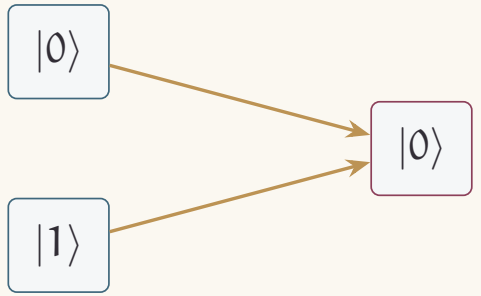
Deutsch–Jozsa offre invece certezza con un solo accesso coerente. La separazione esponenziale appena ricavata riguarda il confronto con il calcolo classico esatto.

Il percorso ha collegato la logica reversibile alla classificazione di una funzione su molte stringhe. Gli approfondimenti successivi conservano dimostrazioni e varianti senza interrompere questa derivazione.

$k \geq 1$: numero di interrogazioni casuali indipendenti con reinserimento. $\mathrm{P}(\text{errore} \mid f \text{ bilanciata})$: probabilità condizionata alla classe bilanciata. La promessa costante/bilanciata rimane valida.

Conservare l'ingresso per ottenere una porta unitaria

Verifichiamo perché l'oracolo conservi l'argomento in un registro. Una porta unitaria conserva i prodotti interni. La regola diretta $|x\rangle \mapsto |f(x)\rangle$ violerebbe questa proprietà per una funzione costante, poiché renderebbe identici due ingressi ortogonali.



due ingressi ortogonali avrebbero la stessa uscita

Prendiamo $f(0) = f(1) = 0$. Prima della trasformazione,

$$\langle 0 \mid 1 \rangle = (1,0)\begin{pmatrix}0\\1\end{pmatrix} = 1\cdot 0 + 0\cdot 1 = 0.$$

Le due uscite coinciderebbero con $|0\rangle$, dunque

$$\langle 0 \mid 0 \rangle = (1,0)\begin{pmatrix}1\\0\end{pmatrix} = 1\cdot 1 + 0\cdot 0 = 1.$$

Per un operatore unitario U, invece,

$$\langle U0 \mid U1 \rangle = \langle 0|U^\dagger U|1\rangle = \langle 0|I_2|1\rangle = \langle 0 \mid 1\rangle = 0.$$

La contraddizione $1 \neq 0$ esclude quella codifica. Conserviamo quindi x in un registro e aggiorniamo un secondo registro.

L'oracolo conserva l'argomento in A. Verifichiamo che applicarlo due volte ripristini entrambi gli ingressi.

$|0\rangle = (1,0)^\mathsf{T}$, $|1\rangle = (0,1)^\mathsf{T}$, $|\pm\rangle = (1,\pm 1)^\mathsf{T}/\sqrt{2}$. $U^\dagger$ è la trasposta coniugata; $U^\dagger U = I_2$ definisce l'unitarietà. $I_2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$.

Applicare due volte l'oracolo ripristina i dati

Nel caso a un bit, con $f : \{0,1\} \to \{0,1\}$, verifichiamo il recupero dell'ingresso applicando due volte lo stesso oracolo. Poiché x resta invariato, il dispositivo usa ancora il medesimo bit $f(x)$; l'algoritmo può eseguire questa seconda chiamata lasciandone ignoto il valore:

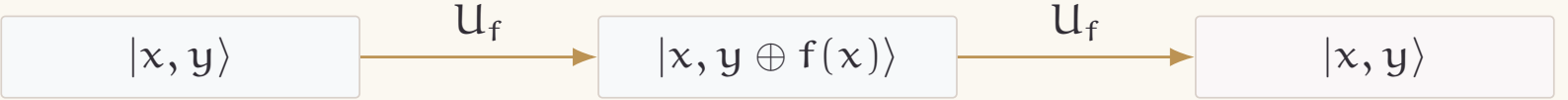
$$\begin{aligned} U_f^2|x,y\rangle &= U_f|x, y \oplus f(x)\rangle \\ &= |x, (y \oplus f(x)) \oplus f(x)\rangle. \end{aligned}$$

Se $f(x) = 0$:

$$(y \oplus 0) \oplus 0 = y \oplus 0 = y.$$

Se $f(x) = 1$:

$$(y \oplus 1) \oplus 1 = (1 - y) \oplus 1 = 1 - (1 - y) = y.$$



Per ogni vettore di base, $U_f^2|x,y\rangle = |x,y\rangle$. Per linearità, $U_f^2 = I_4$ sull'intero spazio e quindi $U_f^{-1} = U_f$.

La trasformazione ripristina ogni vettore della base. Verifichiamo ora l'unitarietà attraverso le colonne della sua matrice.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $I_4 = \mathrm{diag}(1,1,1,1)$. Per un bit y, $y \oplus 1 = 1 - y$. diag elenca gli elementi diagonali, con tutti gli altri nulli.

Le colonne dell'oracolo sono ortonormali

La trasformazione permuta i quattro vettori della base: ogni colonna della matrice contiene un unico 1, in una riga diversa dalle altre colonne. Verifichiamo il prodotto $U_f^\dagger U_f$ attraverso i prodotti interni delle colonne.

colonna j

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

colonna k

$$\begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$1 \cdot 0 + 0 \cdot 1 + 0 \cdot 0 + 0 \cdot 0 = 0$$

Per gli indici di colonna $j, k \in \{0, 1, 2, 3\}$,

$$(U_f^\dagger U_f)_{jk} = \sum_{\ell=0}^{3} (U_f)^*_{\ell j} (U_f)_{\ell k}.$$

Se $j = k$, l'unica componente unitaria contribuisce $1 \cdot 1$:

$$(U_f^\dagger U_f)_{jj} = 1 + 0 + 0 + 0 = 1.$$

Se $j \neq k$, i due 1 occupano righe diverse:

$$(U_f^\dagger U_f)_{jk} = 0 + 0 + 0 + 0 = 0.$$

Otteniamo l'identità I_4, dunque $U_f^\dagger U_f = I_4$. L'oracolo definisce una porta unitaria e può agire su una sovrapposizione normalizzata.

La matrice dell'oracolo è unitaria. Costruiamo ora la matrice della Hadamard sul primo registro, per verificare l'esecuzione sulle quattro componenti.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $U^\dagger$ è la trasposta coniugata: $(U^\dagger)_{j\ell} = U^*_{\ell j}$. $I_4 = \mathrm{diag}(1, 1, 1, 1)$. Una colonna è l'immagine del vettore di base corrispondente.

Costruire la matrice che agisce sul registro congiunto

Per verificare l'esecuzione sulle quattro componenti, costruiamo $H \otimes I_2$: ogni coefficiente di H moltiplica un blocco I_2.

$$H \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1I_2 & 1I_2 \\ 1I_2 & -1I_2 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}.$$

$B = 0$
$|00\rangle, |10\rangle$
ampiezze a, c

$B = 1$
$|01\rangle, |11\rangle$
ampiezze b, e

ogni coppia conserva il secondo indice

Per $v = (a, b, c, e)^T$, svolgiamo le quattro righe:

$$(H \otimes I_2)v = \frac{1}{\sqrt{2}} \begin{pmatrix} 1a + 0b + 1c + 0e \\ 0a + 1b + 0c + 1e \\ 1a + 0b - 1c + 0e \\ 0a + 1b + 0c - 1e \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} a + c \\ b + e \\ a - c \\ b - e \end{pmatrix}.$$

Sommiamo le ampiezze a secondo indice fissato: $|00\rangle$ con $|10\rangle$ per $B = 0$, $|01\rangle$ con $|11\rangle$ per $B = 1$. Il primo indice identifica l'esito della ricombinazione.

La matrice combina ampiezze con lo stesso secondo indice. Applichiamola al vettore prodotto dall'oracolo.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $v = (a, b, c, e)^T$: ampiezze nella base $(00, 01, 10, 11)$. Il prodotto tensoriale sostituisce ogni coefficiente di H con il corrispondente blocco I_2.

La verifica a quattro componenti ritrova la fattorizzazione

Ripartiamo da $w = (s_0, -s_0, s_1, -s_1)^{\mathsf{T}}/2$, con $s_x = (-1)^{f(x)}$. Nel prodotto $(H \otimes I_2)w$, il fattore comune è $1/(2\sqrt{2})$; calcoliamo i quattro numeratori, poi raccogliamo i termini a primo indice fissato:

$$\begin{aligned} n_{00} &= 1s_0 + 0(-s_0) + 1s_1 + 0(-s_1) = s_0 + s_1, \\ n_{01} &= 0s_0 + 1(-s_0) + 0s_1 + 1(-s_1) = -s_0 - s_1, \\ n_{10} &= 1s_0 + 0(-s_0) - 1s_1 + 0(-s_1) = s_0 - s_1, \\ n_{11} &= 0s_0 + 1(-s_0) + 0s_1 - 1(-s_1) = -s_0 + s_1. \end{aligned}$$

$$\begin{aligned} |\Psi_{\text{out}}\rangle &= \frac{(s_0 + s_1)(|00\rangle - |01\rangle)}{2\sqrt{2}} + \frac{(s_0 - s_1)(|10\rangle - |11\rangle)}{2\sqrt{2}} \\ &= \left(\frac{s_0 + s_1}{2}|0\rangle + \frac{s_0 - s_1}{2}|1\rangle \right) \otimes |-\rangle. \end{aligned}$$

$B = 0 : \quad |00\rangle \longleftrightarrow |10\rangle$ $B = 1 : \quad |01\rangle \longleftrightarrow |11\rangle$

Il bersaglio conserva il fattore $|-\rangle$.

La rappresentazione a quattro componenti conferma la fattorizzazione. L'approfondimento seguente ricava gli autovettori della porta X.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $H \otimes I_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$. $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$;

$|x0\rangle - |x1\rangle = |x\rangle \otimes (|0\rangle - |1\rangle) = \sqrt{2}|x\rangle|-\rangle$.

Autovettori e autovalori della porta X

Un vettore $v \neq 0$ è un *autovettore* di X quando $Xv = \lambda v$ per un numero λ, detto *autovalore*. L'operazione restituisce quindi un multiplo del vettore. Ricaviamo tutti i casi:

$$X\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a \end{pmatrix} = \lambda \begin{pmatrix} a \\ b \end{pmatrix} \quad \Longrightarrow \quad b = \lambda a, \quad a = \lambda b.$$

Se $a = 0$, la prima relazione dà $b = 0$, escluso per $v \neq 0$. Poiché $a \neq 0$, possiamo sostituire b e dividere per a:

$$a = \lambda(\lambda a) = \lambda^2 a \quad \Longrightarrow \quad 1 = \lambda^2 \quad \Longrightarrow \quad (\lambda - 1)(\lambda + 1) = 0.$$

Per $\lambda = 1$, $b = a$:

$$v = a\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |+\rangle = \begin{pmatrix} 1 \\ 1 \end{pmatrix}/\sqrt{2}.$$

componenti uguali: $(1, 1) \mapsto (1, 1)$

Per $\lambda = -1$, $b = -a$:

$$v = a\begin{pmatrix} 1 \\ -1 \end{pmatrix}, \qquad |-\rangle = \begin{pmatrix} 1 \\ -1 \end{pmatrix}/\sqrt{2}.$$

componenti opposte: $(1, -1) \mapsto (-1, 1)$

Per $v = (1, \pm 1)^T/\sqrt{2}$, $\|v\|^2 = (1^2 + (\pm 1)^2)/2 = 1$. Gli autovalori $+1$ e -1 descrivono i rispettivi moltiplicatori.

Gli autovalori ±1 caratterizzano gli stati del ritorno di fase. Segue un controllo su ampiezze e probabilità.

$|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$; $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$. $v = (a, b)^T \neq 0$; λ: moltiplicatore nell'equazione $Xv = \lambda v$. $\|(1, \pm 1)^T\| = \sqrt{2}$.

Una norma corretta può nascondere un errore

Per $|\psi\rangle = (2, i)^{\mathsf{T}}/\sqrt{5}$, confrontiamo la proposta $w = (2+i, 2+i)^{\mathsf{T}}/\sqrt{10}$ con il prodotto corretto $v = H|\psi\rangle$. I controlli di norma e probabilità usano gli stessi moduli quadri:

$$|2+i|^2 = (2-i)(2+i) = 4 + 2i - 2i - i^2 = 5,$$
$$|2-i|^2 = (2+i)(2-i) = 4 - 2i + 2i - i^2 = 5.$$

La seconda riga di H richiede $(1 \cdot 2 + (-1)i)/\sqrt{10} = (2-i)/\sqrt{10}$.

$$w = (2+i, 2+i)^{\mathsf{T}}/\sqrt{10}$$

$$p_0(w) = |2+i|^2/10 = 5/10 = 1/2,$$
$$p_1(w) = |2+i|^2/10 = 5/10 = 1/2,$$
$$\|w\|^2 = (5+5)/10 = 1.$$

$$v = (2+i, 2-i)^{\mathsf{T}}/\sqrt{10}$$

$$p_0(v) = |2+i|^2/10 = 5/10 = 1/2,$$
$$p_1(v) = |2-i|^2/10 = 5/10 = 1/2,$$
$$\|v\|^2 = (5+5)/10 = 1.$$

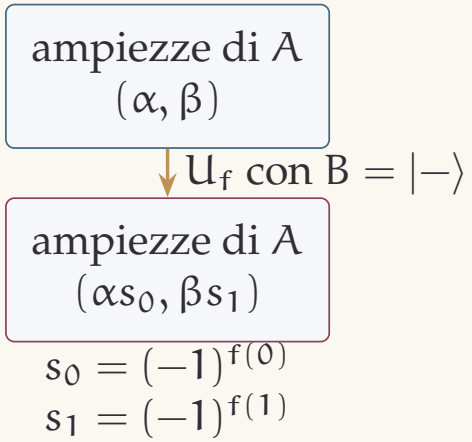
L'esempio mostra perché il controllo di una simulazione debba confrontare anche le ampiezze. Le varianti seguenti studiano preparazioni diverse dei registri.

BASE $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$; $(a,b)^{\mathsf{T}} = a|0\rangle + b|1\rangle$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$. $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$. $i^2 = -1$, $i^* = -i$; * indica il coniugato. Prima componente corretta: $v_0 = (1 \cdot 2 + 1 \cdot i)/\sqrt{10} = (2+i)/\sqrt{10}$.

Il ritorno di fase vale anche per ampiezze arbitrarie

Per una funzione a un bit variamo la preparazione di A: scegliamo $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$, con $|\alpha|^2 + |\beta|^2 = 1$, e il bersaglio $|-\rangle$. Definiamo $s_0 = (-1)^{f(0)}$ e $s_1 = (-1)^{f(1)}$. Ciascun segno vale $+1$ oppure -1.

$$\begin{aligned} U_f(|\chi\rangle|-\rangle) &= U_f\big(\alpha|0\rangle|-\rangle + \beta|1\rangle|-\rangle\big) \\ &= \alpha U_f(|0\rangle|-\rangle) + \beta U_f(|1\rangle|-\rangle) \\ &= \alpha s_0|0\rangle|-\rangle + \beta s_1|1\rangle|-\rangle \\ &= (\alpha s_0|0\rangle + \beta s_1|1\rangle) \otimes |-\rangle. \end{aligned}$$



Il primo fattore è $|\chi'\rangle = \alpha s_0|0\rangle + \beta s_1|1\rangle$; il bersaglio resta $|-\rangle$.
L'oracolo moltiplica ciascuna ampiezza per il segno determinato da f: è il *ritorno di fase*.

$$\||\chi'\rangle\|^2 = |\alpha s_0|^2 + |\beta s_1|^2 = |\alpha|^2 \cdot 1 + |\beta|^2 \cdot 1 = 1.$$

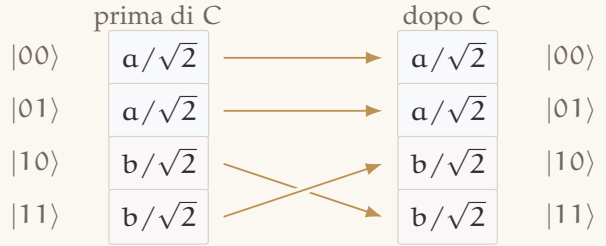
La norma del primo registro si conserva perché $|s_0|^2 = |s_1|^2 = 1$.

La stessa regola di fase vale per ampiezze arbitrarie. Confrontiamo ora gli ausiliari più e meno nella CNOT.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $s_x = (-1)^{f(x)}$; $(-1)^0 = 1$, $(-1)^1 = -1$. $|\chi\rangle = \alpha|0\rangle + \beta|1\rangle$; $|\alpha|^2 + |\beta|^2 = 1$. $|s_x|^2 = 1$.

CNOT con il bersaglio nello stato $|+\rangle$

Riprendiamo CNOT con controllo $|\chi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$, e bersaglio $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$. Calcoliamo prima $X|+\rangle$, poiché la CNOT applica questo scambio nel ramo con controllo uno.



$\chi = (a, b)^T$: coefficienti del controllo. Il bersaglio $|+\rangle$ rende uguali le due ampiezze scambiate.

$$X|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle.$$

$$C|0\rangle|+\rangle = |0\rangle \otimes I_2|+\rangle = |0\rangle|+\rangle, \quad C|1\rangle|+\rangle = |1\rangle \otimes X|+\rangle = |1\rangle|+\rangle.$$

$$\begin{aligned} C(|\chi\rangle \otimes |+\rangle) &= C\big(a|0\rangle|+\rangle + b|1\rangle|+\rangle\big) \\ &= aC|0\rangle|+\rangle + bC|1\rangle|+\rangle \\ &= a|0\rangle|+\rangle + b|1\rangle|+\rangle \\ &= (a|0\rangle + b|1\rangle) \otimes |+\rangle = |\chi\rangle \otimes |+\rangle. \end{aligned}$$

Nell'ingresso $(a|00\rangle + a|01\rangle + b|10\rangle + b|11\rangle)/\sqrt{2}$, le due componenti scambiate hanno entrambe ampiezza $b/\sqrt{2}$.

Entrambi i rami conservano lo stesso bersaglio e l'intero stato resta invariato. Cambiamo ora soltanto il segno relativo del bersaglio, mantenendo lo stesso controllo.

DATI E REGOLE $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $C|xy\rangle = |x, y \oplus x\rangle$; $00 \mapsto 00$, $01 \mapsto 01$, $10 \mapsto 11$, $11 \mapsto 10$. $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $\chi = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$.

CNOT con il bersaglio nello stato $|-\rangle$

Manteniamo $|\chi\rangle = a|0\rangle + b|1\rangle$, $|a|^2 + |b|^2 = 1$, e prepariamo il bersaglio $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Lo scambio di due ampiezze opposte produce un segno nel ramo con controllo uno.

$$X|-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 0\cdot 1 + 1(-1) \\ 1\cdot 1 + 0(-1) \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = -\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = -|-\rangle.$$

	prima di C			dopo C	
	$y=0$	$y=1$		$y=0$	$y=1$
$x=0$	a	$-a$	$x=0$	a	$-a$
$x=1$	b	$-b$	$x=1$	$-b$	b

Ogni cella è moltiplicata per $1/\sqrt{2}$.

Per linearità,

$$\begin{aligned} C(|\chi\rangle \otimes |-\rangle) &= a|0\rangle \otimes I_2|-\rangle + b|1\rangle \otimes X|-\rangle \\ &= a|0\rangle \otimes |-\rangle + b|1\rangle \otimes (-|-\rangle) \\ &= (a|0\rangle - b|1\rangle) \otimes |-\rangle. \end{aligned}$$

La raccolta del fattore comune è esplicita anche in componenti:

$$\frac{a|00\rangle - a|01\rangle + b|11\rangle - b|10\rangle}{\sqrt{2}} = \frac{a|0\rangle \otimes (|0\rangle - |1\rangle) - b|1\rangle \otimes (|0\rangle - |1\rangle)}{\sqrt{2}}.$$

Il coefficiente b cambia segno e il bersaglio resta $|-\rangle$. Se $a, b \neq 0$, cambia la fase relativa del controllo. Per $a = 0$ cambia soltanto una fase globale; per $b = 0$ il vettore resta identico. Verifichiamo il confronto con dati numerici.

DATI E REGOLE $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. $C|xy\rangle = |x, y \oplus x\rangle$; $00 \mapsto 00$, $01 \mapsto 01$, $10 \mapsto 11$, $11 \mapsto 10$. $|\pm\rangle = (1, \pm 1)^{\mathsf{T}}/\sqrt{2}$. a, b: ampiezze del controllo; $|a|^2 + |b|^2 = 1$.

Il bersaglio più sullo stato numerico

Usiamo $|\chi\rangle = (2, i)^T/\sqrt{5}$ e $|+\rangle = (1, 1)^T/\sqrt{2}$. Espandiamo il prodotto prima della CNOT: le posizioni 10 e 11 permettono di verificare con coefficienti complessi l'invarianza già dimostrata in forma generale.

prima e dopo; fattore $1/\sqrt{10}$

	$y=0$	$y=1$
$x=0$	2	2
$x=1$	i	i

$$|\chi\rangle|+\rangle = \frac{1}{\sqrt{10}}(2\cdot 1, 2\cdot 1, i\cdot 1, i\cdot 1)^T = \frac{1}{\sqrt{10}}(2, 2, i, i)^T.$$

$$C|\chi\rangle|+\rangle = \frac{1}{\sqrt{10}}\begin{pmatrix} 1\cdot 2+0\cdot 2+0\cdot i+0\cdot i \\ 0\cdot 2+1\cdot 2+0\cdot i+0\cdot i \\ 0\cdot 2+0\cdot 2+0\cdot i+1\cdot i \\ 0\cdot 2+0\cdot 2+1\cdot i+0\cdot i \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2 \\ 2 \\ i \\ i \end{pmatrix} = |\chi\rangle|+\rangle.$$

La norma quadrata è $(4+4+1+1)/10 = 10/10 = 1$. Il controllo resta nello stato $|\chi\rangle$.

Le componenti scambiate coincidono, quindi il vettore resta invariato. La preparazione nello stato meno introdurrà coefficienti opposti proprio nelle due posizioni coinvolte.

DATI E REGOLE Base $(00, 01, 10, 11)$; $C(v_{00}, v_{01}, v_{10}, v_{11})^T = (v_{00}, v_{01}, v_{11}, v_{10})^T$. $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$; $i^2 = -1$, $i^* = -i$, $|z|^2 = z^* z$. $(a, b)^T \otimes (c, d)^T = (ac, ad, bc, bd)^T$.

Il bersaglio meno sullo stato numerico

Per $|\chi\rangle = (2, i)^T/\sqrt{5}$ e $|-\rangle = (1, -1)^T/\sqrt{2}$, la CNOT scambia 10, 11. La fattorizzazione identifica il nuovo controllo.

$$|\chi\rangle|-\rangle = \frac{(2\cdot 1, 2\cdot(-1), i\cdot 1, i\cdot(-1))^T}{\sqrt{10}} = \frac{(2, -2, i, -i)^T}{\sqrt{10}}.$$

uscita; fattore $1/\sqrt{10}$

	$y=0$	$y=1$
$x=0$	2	-2
$x=1$	$-i$	i

$$C|\chi\rangle|-\rangle = \frac{1}{\sqrt{10}}\begin{pmatrix} 1\cdot 2 + 0(-2) + 0i + 0(-i) \\ 0\cdot 2 + 1(-2) + 0i + 0(-i) \\ 0\cdot 2 + 0(-2) + 0i + 1(-i) \\ 0\cdot 2 + 0(-2) + 1i + 0(-i) \end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix} 2 \\ -2 \\ -i \\ i \end{pmatrix}.$$

$$\frac{(2, -2, -i, i)^T}{\sqrt{10}} = \frac{2|0\rangle \otimes (|0\rangle - |1\rangle) - i|1\rangle \otimes (|0\rangle - |1\rangle)}{\sqrt{10}}$$

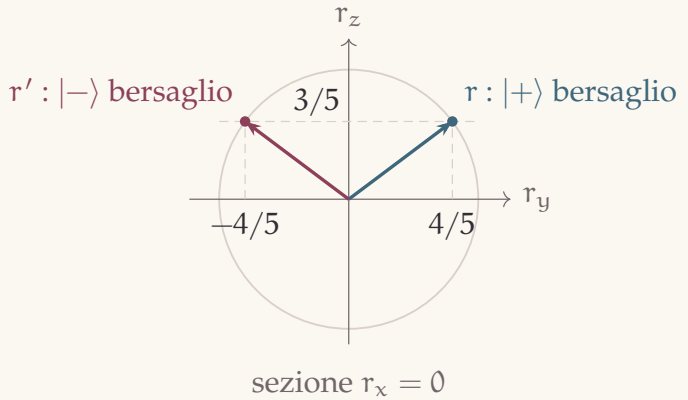
$$= \frac{(2|0\rangle - i|1\rangle) \otimes (|0\rangle - |1\rangle)}{\sqrt{5}\sqrt{2}} = \frac{2|0\rangle - i|1\rangle}{\sqrt{5}}|-\rangle.$$

Il controllo passa da $(2, i)^T/\sqrt{5}$ a $(2, -i)^T/\sqrt{5}$, mentre il bersaglio conserva $|-\rangle$. La norma quadrata resta $(4+4+1+1)/10 = 10/10 = 1$; la geometria confronterà ora i due effetti.

DATI E REGOLE Base $(00, 01, 10, 11)$; $C(v_{00}, v_{01}, v_{10}, v_{11})^T = (v_{00}, v_{01}, v_{11}, v_{10})^T$. $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$; $i^2 = -1$, $i^* = -i$, $|z|^2 = z^* z$. $(a, b)^T \otimes (c, d)^T = (ac, ad, bc, bd)^T$.

Due bersagli, due effetti sul controllo

Con controllo iniziale $(2, i)^T/\sqrt{5}$, entrambi i bersagli hanno lasciato il registro fattorizzato. Rappresentiamo quindi il primo qubit sulla sfera: il confronto delle coordinate individua la differenza prodotta dalla preparazione del bersaglio.



sezione $r_x = 0$

Sezione del controllo, il cui stato è puro perché l'uscita si fattorizza.

Con bersaglio $|+\rangle$, il controllo resta $(2, i)^T/\sqrt{5}$:

$$a^* b = (2/\sqrt{5})(i/\sqrt{5}) = 2i/5,$$
$$r = (2 \cdot 0, 2 \cdot 2/5, 4/5 - 1/5) = (0, 4/5, 3/5).$$

Con bersaglio $|-\rangle$, il controllo diventa $(2, -i)^T/\sqrt{5}$:

$$a'^* b' = (2/\sqrt{5})(-i/\sqrt{5}) = -2i/5,$$
$$r' = (2 \cdot 0, 2 \cdot (-2/5), 4/5 - 1/5) = (0, -4/5, 3/5).$$

Per entrambi, $p_0 = |2/\sqrt{5}|^2 = 2^2/5 = 4/5$ e $p_1 = |\pm i/\sqrt{5}|^2 = (\mp i)(\pm i)/5 = -i^2/5 = 1/5$.

La scelta dello stato del bersaglio cambia l'effetto sulle fasi del controllo. Verifichiamo il circuito di Deutsch quando anche il bersaglio viene preparato nello stato più.

DATI E REGOLE $r = (2\,\mathrm{Re}(a^* b), 2\,\mathrm{Im}(a^* b), |a|^2 - |b|^2)$ per lo stato normalizzato $(a, b)^T$; $p_0 = |a|^2$, $p_1 = |b|^2$; $|z|^2 = z^* z$; $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$.

Il bersaglio più lascia invariato lo stato per ogni funzione

Nel circuito di Deutsch manteniamo A in $|+\rangle$ e poniamo B in $|+\rangle$ per isolare il ruolo del segno relativo. La preparazione $|+\rangle_A|+\rangle_B$ si ottiene da $|00\rangle$. Poiché $H|0\rangle = (1\cdot 1 + 1\cdot 0, 1\cdot 1 - 1\cdot 0)^T/\sqrt{2} = (1,1)^T/\sqrt{2}$,

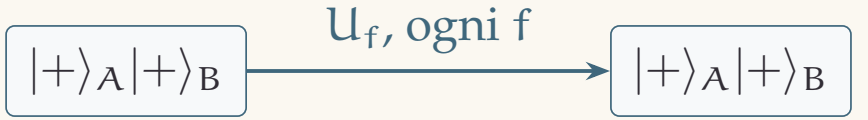
$$(H\otimes H)|00\rangle = \frac{1}{2}\begin{pmatrix}1\\1\end{pmatrix}\otimes\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{2}(1\cdot 1, 1\cdot 1, 1\cdot 1, 1\cdot 1)^T = \frac{1}{2}(1,1,1,1)^T.$$

La norma quadrata è $4(1/2)^2 = 4/4 = 1$. Le due azioni possibili sul bersaglio danno lo stesso risultato:

$$I_2|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\cdot 1 + 0\cdot 1\\ 0\cdot 1 + 1\cdot 1\end{pmatrix} = |+\rangle, \qquad X|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\cdot 1 + 1\cdot 1\\ 1\cdot 1 + 0\cdot 1\end{pmatrix} = |+\rangle.$$

Quindi $U_f(|x\rangle|+\rangle) = |x\rangle|+\rangle$ per ogni x e per entrambi i valori di $f(x)$. Per linearità,

$$U_f\,\frac{|0\rangle|+\rangle + |1\rangle|+\rangle}{\sqrt{2}} = \frac{U_f(|0\rangle|+\rangle) + U_f(|1\rangle|+\rangle)}{\sqrt{2}} = \frac{|0\rangle|+\rangle + |1\rangle|+\rangle}{\sqrt{2}} = |+\rangle|+\rangle.$$



L'oracolo lascia lo stesso vettore per tutte le funzioni. La Hadamard finale produrrà quindi la stessa lettura.

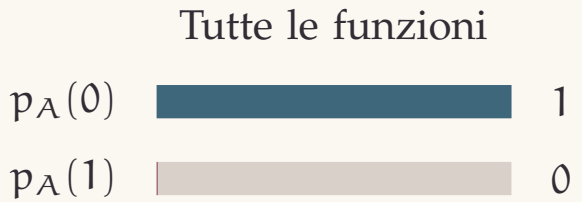
A: primo qubit; B: bersaglio; $|xy\rangle = |x\rangle\otimes|y\rangle$. Base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$, $I_2 = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$, $X = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. $U_f|x,y\rangle = |x, y\oplus f(x)\rangle$; estensione per linearità alle sovrapposizioni.

Bersaglio più: la lettura restituisce sempre zero

Ripartiamo dallo stato $v = (1,1,1,1)^{\mathsf{T}}/2$, comune a tutti gli oracoli con il bersaglio in $|+\rangle$. Proviamo ad applicare H al primo registro per combinarne le ampiezze prima della misura. Svolgiamo ogni prodotto di riga:

$$(H \otimes I_2)v = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \frac{1}{2\sqrt{2}} \begin{pmatrix} 1\cdot 1 + 0\cdot 1 + 1\cdot 1 + 0\cdot 1 \\ 0\cdot 1 + 1\cdot 1 + 0\cdot 1 + 1\cdot 1 \\ 1\cdot 1 + 0\cdot 1 - 1\cdot 1 + 0\cdot 1 \\ 0\cdot 1 + 1\cdot 1 + 0\cdot 1 - 1\cdot 1 \end{pmatrix}$$

$$= \frac{(2,2,0,0)^{\mathsf{T}}}{2\sqrt{2}} = \frac{(1,1,0,0)^{\mathsf{T}}}{\sqrt{2}} = |0\rangle|+\rangle.$$



$$p_A(0) = |1/\sqrt{2}|^2 + |1/\sqrt{2}|^2 = \tfrac{1}{2} + \tfrac{1}{2} = 1,$$
$$p_A(1) = |0|^2 + |0|^2 = 0.$$

Per l'identità, $f(0) = 0$, $f(1) = 1$, servirebbe $d = 0 \oplus 1 = 1$; otteniamo invece zero. Il bersaglio $|+\rangle$ ha autovalore $+1$ sia per I_2 sia per X, perciò le due azioni lasciano la stessa traccia.

Il bersaglio più dà sempre zero. Confrontiamo ora l'ingresso zero dell'ausiliario e le correlazioni che produce.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$, $|\pm\rangle = (1,\pm 1)^{\mathsf{T}}/\sqrt{2}$. $p(x,y) = |c_{xy}|^2$; $p_A(x) = p(x,0) + p(x,1)$; $|z|^2 = z^* z$. $H \otimes I_2$ è la matrice esplicitata nel calcolo. $X|+\rangle = |+\rangle$; $X|-\rangle = -|-\rangle$.

Bersaglio zero: il risultato è uno stato congiunto

Proviamo a registrare direttamente il valore della funzione in B, inizializzandolo a zero. Scegliamo $f(x) = x$, così l'oracolo è la CNOT già nota, e prepariamo $|+\rangle_A = (|0\rangle + |1\rangle)/\sqrt{2}$, $|0\rangle_B$. Applichiamo la linearità ai due contributi:

$$U_f(|+\rangle|0\rangle) = U_f \frac{|00\rangle + |10\rangle}{\sqrt{2}} = \frac{U_f|00\rangle + U_f|10\rangle}{\sqrt{2}}$$
$$= \frac{|0, 0 \oplus 0\rangle + |1, 0 \oplus 1\rangle}{\sqrt{2}} = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Ampiezze del singolo stato congiunto

$\lvert 00\rangle$	$\lvert 01\rangle$	$\lvert 10\rangle$	$\lvert 11\rangle$
$c_{00} = 1/\sqrt{2}$	$c_{01} = 0$	$c_{10} = 0$	$c_{11} = 1/\sqrt{2}$

Ogni termine associa ingresso e valore della funzione. La norma quadrata è $|1/\sqrt{2}|^2 + 0 + 0 + |1/\sqrt{2}|^2 = 1/2 + 0 + 0 + 1/2 = 1$. L'uscita è la coppia di Bell, stato congiunto dei registri A e B.

La misura successiva stabilirà quanta informazione sull'associazione ingresso–valore sia accessibile in una singola esecuzione.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $|+\rangle|0\rangle = (|00\rangle + |10\rangle)/\sqrt{2}$; $\|v\|^2$ è la somma dei moduli quadri delle componenti.

La misura immediata restituisce una sola coppia

Per l'identità, l'ingresso $|+\rangle|0\rangle$ ha prodotto $|\Psi\rangle = (1,0,0,1)^{\mathsf{T}}/\sqrt{2}$. Calcoliamo separatamente i quattro pesi della misura nella base congiunta:

$$p(0,0) = |1/\sqrt{2}|^2 = 1/2, \quad p(0,1) = |0|^2 = 0,$$
$$p(1,0) = |0|^2 = 0, \quad p(1,1) = |1/\sqrt{2}|^2 = 1/2.$$

	$B=0$	$B=1$
$A=0$	$p(0,0)=1/2$	$p(0,1)=0$
$A=1$	$p(1,0)=0$	$p(1,1)=1/2$

La somma $1/2+0+0+1/2=1$ verifica la normalizzazione. Ogni misura restituisce 00 oppure 11. L'esito 00 rivela $f(0)=0$, compatibile anche con la costante zero. L'esito 11 rivela $f(1)=1$, compatibile anche con la costante uno.

Questa preparazione seguita dalla misura della base lascia quindi ambigua la classe. Il confronto chiarisce la funzione del bersaglio meno e della ricombinazione finale nel circuito di Deutsch già svolto.

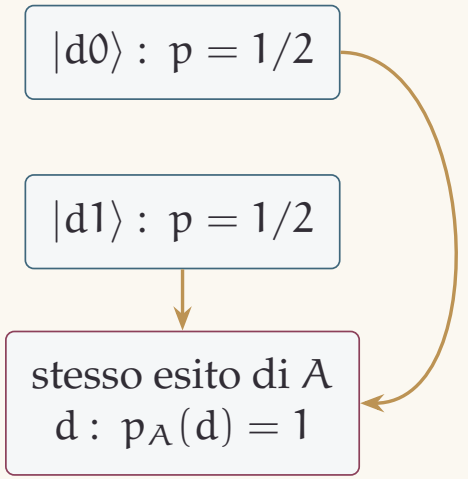
Una singola coppia osservata rimane compatibile con una funzione costante e una bilanciata. Torniamo al circuito riuscito per descrivere la sua misura selettiva.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00,01,10,11)$. $|0\rangle = (1,0)^{\mathsf{T}}$, $|1\rangle = (0,1)^{\mathsf{T}}$, $|\pm\rangle = (1,\pm1)^{\mathsf{T}}/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0\oplus0 = 1\oplus1 = 0$, $0\oplus1 = 1\oplus0 = 1$. $p(x,y) = |c_{xy}|^2$; $p_A(x) = p(x,0) + p(x,1)$; $|z|^2 = z^*z$.

Misurare il primo registro e conservare il bersaglio

Ripartiamo da $|\Psi_{\text{out}}\rangle = \eta|d\rangle|-\rangle = (\eta|d0\rangle - \eta|d1\rangle)/\sqrt{2}$, con $\eta = \pm 1$ e $d = f(0) \oplus f(1)$. I due termini hanno lo stesso primo indice:

$$p(d,0) = |\eta/\sqrt{2}|^2 = \eta^2/2 = \tfrac{1}{2}, \qquad p(d,1) = |-\eta/\sqrt{2}|^2 = (-\eta)^2/2 = \tfrac{1}{2},$$
$$p_A(d) = \tfrac{1}{2} + \tfrac{1}{2} = 1, \qquad p_A(1-d) = 0 + 0 = 0.$$



Poiché $\langle d||d\rangle = 1$, il proiettore $P_d = |d\rangle\langle d| \otimes I_2$ conserva ciascun termine con primo indice d:

$$P_d|\Psi_{\text{out}}\rangle = \frac{\eta \cdot 1|d0\rangle - \eta \cdot 1|d1\rangle}{\sqrt{2}} = |\Psi_{\text{out}}\rangle.$$

Normalizziamo dividendo per la radice della probabilità dell'esito:

$$|\Psi_d\rangle = \frac{P_d|\Psi_{\text{out}}\rangle}{\sqrt{p_A(d)}} = \frac{|\Psi_{\text{out}}\rangle}{\sqrt{1}} = |\Psi_{\text{out}}\rangle.$$

Il bersaglio conserva $|-\rangle$.

La misura certa del primo registro conserva l'ausiliario. Gli esempi successivi variano le ampiezze iniziali, mantenendo esplicite tutte le probabilità.

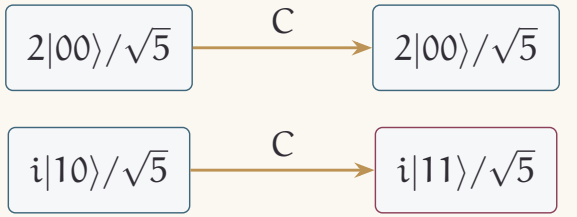
REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $j \in \{0,1\}$; $P_j = |j\rangle\langle j| \otimes I_2$. Per $p_A(j) > 0$, lo stato condizionato è $P_j|\Psi\rangle/\sqrt{p_A(j)}$.

Ingresso complesso: applicare l'oracolo al registro

Per studiare il ruolo della preparazione di A, riprendiamo $|\chi\rangle = (2|0\rangle + i|1\rangle)/\sqrt{5}$: rispetto a $|+\rangle$ cambiano insieme i moduli e la fase relativa. Fissiamo $f(x) = x$, quindi U_f è CNOT. Confrontiamo B in $|0\rangle$ e in $|-\rangle$, iniziando da $|\chi\rangle|0\rangle_B$. La norma è $(|2|^2 + |i|^2)/5 = (4+1)/5 = 1$.

$$|\chi\rangle \otimes |0\rangle = \frac{1}{\sqrt{5}}(2, i)^T \otimes (1, 0)^T = \frac{1}{\sqrt{5}}(2\cdot 1, 2\cdot 0, i\cdot 1, i\cdot 0)^T = \frac{1}{\sqrt{5}}(2, 0, i, 0)^T.$$

$$U_f|\chi, 0\rangle = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 2 \\ 0 \\ i \\ 0 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 1\cdot 2 + 0\cdot 0 + 0i + 0\cdot 0 \\ 0\cdot 2 + 1\cdot 0 + 0i + 0\cdot 0 \\ 0\cdot 2 + 0\cdot 0 + 0i + 1\cdot 0 \\ 0\cdot 2 + 0\cdot 0 + 1i + 0\cdot 0 \end{pmatrix} = \frac{1}{\sqrt{5}} \begin{pmatrix} 2 \\ 0 \\ 0 \\ i \end{pmatrix}.$$



L'uscita $|\Psi\rangle = (2|00\rangle + i|11\rangle)/\sqrt{5}$ conserva il coefficiente i, trasferendolo da 10 a 11.

Calcoliamo le probabilità e verifichiamo la fattorizzazione del risultato, così da interpretare correttamente i due registri.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$. $i^2 = -1$, $i^* = -i$, $|i|^2 = (-i)i = 1$. Il prodotto tensoriale ordina le componenti come (ac, ae, bc, be).

Ingresso complesso: probabilità e correlazioni

Per $f(x) = x$, l'ingresso $(2|0\rangle + i|1\rangle)|0\rangle/\sqrt{5}$ ha prodotto $|\Psi\rangle = (2, 0, 0, i)^T/\sqrt{5}$. Applichiamo Born usando il coniugato dell'ampiezza complessa:

$$p(0,0) = \left|2/\sqrt{5}\right|^2 = 4/5, \quad p(0,1) = |0|^2 = 0,$$

$$p(1,0) = |0|^2 = 0, \qquad p(1,1) = \left|i/\sqrt{5}\right|^2 = \frac{(-i)i}{5} = \frac{-i^2}{5} = 1/5.$$

	$B = 0$	$B = 1$
$A = 0$	$p(0,0) = 4/5$	$p(0,1) = 0$
$A = 1$	$p(1,0) = 0$	$p(1,1) = 1/5$

La somma dei pesi è $4/5 + 0 + 0 + 1/5 = 1$. L'esito 00 resta compatibile con la costante zero; 11 resta compatibile con la costante uno.

Per una fattorizzazione servirebbe

$$(a|0\rangle + b|1\rangle)(c|0\rangle + e|1\rangle) = ac|00\rangle + ae|01\rangle + bc|10\rangle + be|11\rangle,$$

$$ac = 2/\sqrt{5}, \quad ae = 0, \quad bc = 0, \quad be = i/\sqrt{5}.$$

Le relazioni $ac \neq 0$ e $be \neq 0$ impongono $a, b, c, e \neq 0$, quindi $ae \neq 0$ e $bc \neq 0$: contraddizione.

Lo stato è entangled; la griglia descrive probabilità congiunte dei due registri.

Manteniamo A e cambiamo soltanto B da zero a meno, per confrontare correlazioni e ritorno di fase.

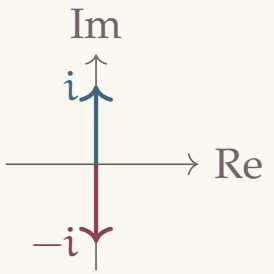
REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $p(x,y) = |c_{xy}|^2$; $p_A(x) = p(x,0) + p(x,1)$; $|z|^2 = z^* z$. $i^* = -i$, $i^2 = -1$. a, b, c, e sono coefficienti ipotetici di un prodotto; il loro confronto verifica la separabilità.

Lo stesso ingresso complesso con bersaglio meno

Per la stessa identità $f(0) = 0$, $f(1) = 1$, cambiamo soltanto B. Prepariamo $|\chi\rangle = (2|0\rangle + i|1\rangle)/\sqrt{5}$ e $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. I fattori sono $s_0 = (-1)^0 = 1$ e $s_1 = (-1)^1 = -1$. Per linearità:

$$\begin{aligned} U_f(|\chi\rangle|-\rangle) &= \big[2U_f(|0\rangle|-\rangle) + iU_f(|1\rangle|-\rangle)\big]/\sqrt{5} \\ &= \big[(2\cdot 1)|0\rangle|-\rangle + i(-1)|1\rangle|-\rangle\big]/\sqrt{5} \\ &= \big[(2|0\rangle - i|1\rangle)/\sqrt{5}\big] \otimes |-\rangle. \end{aligned}$$

Il bersaglio resta $|-\rangle$; il coefficiente i diventa $-i$.



numeratore: $i \mapsto -i$

Le quattro componenti si ottengono dal prodotto tensoriale:

$$\frac{(2,-i)^T \otimes (1,-1)^T}{\sqrt{10}} = \frac{(2\cdot 1,\, 2(-1),\, (-i)\cdot 1,\, (-i)(-1))^T}{\sqrt{10}} = \frac{(2,-2,-i,i)^T}{\sqrt{10}}.$$

La norma del primo registro è $(|2|^2 + |-i|^2)/5 = (4 + i(-i))/5 = (4 - i^2)/5 = 1$; quella del vettore congiunto è $(4+4+1+1)/10 = 1$.

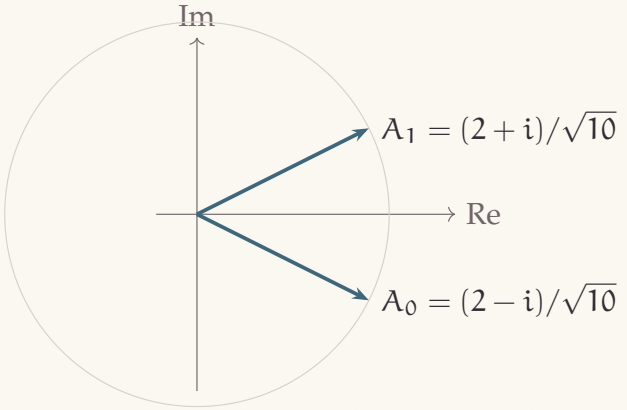
Completiamo la Hadamard sul primo registro e calcoliamo la distribuzione di questa preparazione.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1,\pm 1)^T/\sqrt{2}$. $U_f|xy\rangle = |x, y \oplus f(x)\rangle$; XOR: $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$. $U_f|x\rangle|-\rangle = (-1)^{f(x)}|x\rangle|-\rangle$; $i^2 = -1$, $i^* = -i$, $(-i)^* = i$. Il diagramma indica i numeratori delle ampiezze.

Hadamard combina le ampiezze complesse

Per $f(x) = x$, l'ingresso $(2|0\rangle + i|1\rangle)|-\rangle/\sqrt{5}$ ha prodotto $(2|0\rangle - i|1\rangle)|-\rangle/\sqrt{5}$. Hadamard agisce sul primo fattore:

$$H\frac{1}{\sqrt{5}}\begin{pmatrix}2\\-i\end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\begin{pmatrix}2\\-i\end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix}1\cdot 2 + 1(-i)\\1\cdot 2 - 1(-i)\end{pmatrix} = \frac{1}{\sqrt{10}}\begin{pmatrix}2-i\\2+i\end{pmatrix}.$$



ampiezze nel piano complesso
raggio $1/\sqrt{2}$, modulo quadro $1/2$

Lo stato congiunto risultante è

$$\left(\frac{2-i}{\sqrt{10}}|0\rangle + \frac{2+i}{\sqrt{10}}|1\rangle\right) \otimes |-\rangle.$$

Le ampiezze sono coniugate e hanno uguale lunghezza. Entrambe conservano una parte reale diversa da zero, quindi la ricombinazione lascia presenti i due esiti.

Il modulo quadro di ciascuna ampiezza fornirà la probabilità della risposta corrispondente.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}$, $I_2 = \begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}$. $i^2 = -1$.

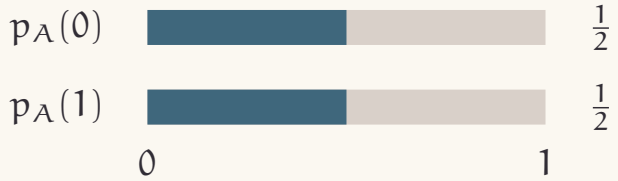
$A_0 = (2-i)/\sqrt{10}$, $A_1 = (2+i)/\sqrt{10}$ sono ampiezze del primo registro; il grafico è nel piano complesso delle ampiezze.

La preparazione iniziale determina la certezza della lettura

Per l'identità, l'esempio complesso ha dato $A_0 = (2-i)/\sqrt{10}$ e $A_1 = (2+i)/\sqrt{10}$. Sviluppiamo i prodotti con i coniugati:

$$\begin{aligned} p_A(0) = |A_0|^2 &= \frac{(2+i)(2-i)}{10} = \frac{2\cdot 2 + 2(-i) + i\cdot 2 + i(-i)}{10} \\ &= (4 - 2i + 2i - i^2)/10 = (4+1)/10 = 1/2, \\ p_A(1) = |A_1|^2 &= \frac{(2-i)(2+i)}{10} = \frac{2\cdot 2 + 2i + (-i)2 + (-i)i}{10} \\ &= (4 + 2i - 2i - i^2)/10 = (4+1)/10 = 1/2. \end{aligned}$$

Esempio complesso



La somma dei pesi è $1/2 + 1/2 = 1$. Questa funzione richiede $d = 1$; il circuito produce anche zero con probabilità $1/2$.

Preparando A in $|+\rangle$ e mantenendo B in $|-\rangle$, l'esito errato ha ampiezza nulla per cancellazione.

Lo stato meno dell'ausiliario produce ancora il ritorno di fase. La preparazione scelta per A conserva però due esiti dopo H e perde la certezza della lettura; moduli e fase sono stati modificati insieme.

REGISTRI A: primo qubit; B: bersaglio. $|xy\rangle = |x\rangle \otimes |y\rangle$; base $(00, 01, 10, 11)$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$, $|\pm\rangle = (1, \pm 1)^T/\sqrt{2}$. $p_A(j) = |A_j|^2$; $|z|^2 = z^* z$; $(2 \pm i)^* = 2 \mp i$, $i^2 = -1$. Il bersaglio normalizzato resta fattorizzato.

Preparare il calcolo coerente di AND

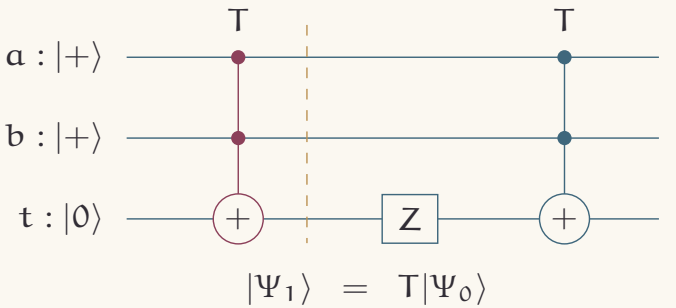
Vogliamo assegnare un segno meno al termine con $a = b = 1$, mantenendo infine l'ausiliario in zero. Prepariamo $|\Psi_0\rangle = |+\rangle|+\rangle|0\rangle$ e sviluppiamo il prodotto:

$$|\Psi_0\rangle = \frac{(|0\rangle + |1\rangle)(|0\rangle + |1\rangle)|0\rangle}{2} = \frac{|000\rangle + |010\rangle + |100\rangle + |110\rangle}{2}.$$

Calcoliamo AND su ciascuna componente:

$$\begin{aligned} T|000\rangle &= |00, 0 \oplus (0 \cdot 0)\rangle = |000\rangle, \\ T|010\rangle &= |01, 0 \oplus (0 \cdot 1)\rangle = |010\rangle, \\ T|100\rangle &= |10, 0 \oplus (1 \cdot 0)\rangle = |100\rangle, \\ T|110\rangle &= |11, 0 \oplus (1 \cdot 1)\rangle = |111\rangle. \end{aligned}$$

Per linearità, $|\Psi_1\rangle = (|000\rangle + |010\rangle + |100\rangle + |111\rangle)/2$.



La sezione evidenzia lo stato dopo la prima Toffoli.

Prima e dopo Toffoli, la norma quadrata è $4 \cdot |1/2|^2 = 1$. Il valore di AND può ora controllare la fase.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $|0\rangle = (1, 0)^T$, $|1\rangle = (0, 1)^T$; $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$.

Usare il risultato di AND per assegnare una fase

Ripartiamo da $|\Psi_1\rangle = (|000\rangle + |010\rangle + |100\rangle + |111\rangle)/2$. L'ausiliario contiene AND. La porta Z_t usa quel valore per cambiare il segno del contributo con terzo indice uno:

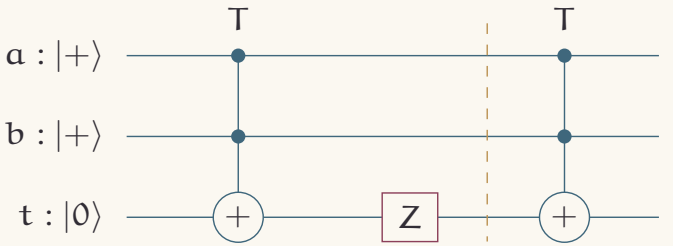
$$Z|0\rangle = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 \\ 0\cdot 1 - 1\cdot 0 \end{pmatrix} = |0\rangle, \qquad Z|1\rangle = \begin{pmatrix} 1\cdot 0 + 0\cdot 1 \\ 0\cdot 0 - 1\cdot 1 \end{pmatrix} = -|1\rangle.$$

Sul registro completo,

$$Z_t|000\rangle = |000\rangle, \quad Z_t|010\rangle = |010\rangle,$$
$$Z_t|100\rangle = |100\rangle, \quad Z_t|111\rangle = -|111\rangle.$$

Per linearità,

$$|\Psi_2\rangle = Z_t|\Psi_1\rangle = \frac{|000\rangle + |010\rangle + |100\rangle - |111\rangle}{2}.$$



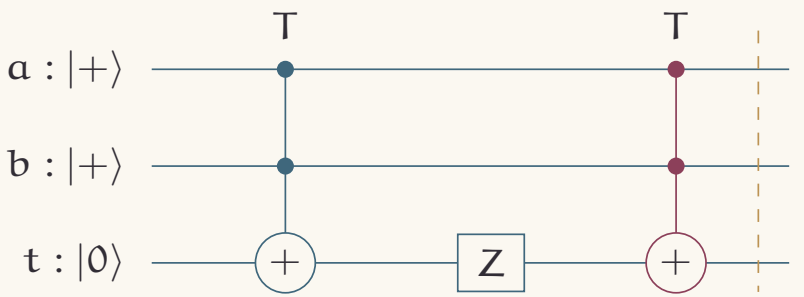
Z_t agisce sul terzo qubit. Il segno resta associato al contributo selezionato.

La norma è $(1+1+1+1)/4 = 1$. Applichiamo la seconda Toffoli per ripristinare l'ausiliario.

$T|a,b,t\rangle = |a,b,t\oplus ab\rangle$; $a,b,t \in \{0,1\}$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $j = 4a + 2b + t$. $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$; $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z_t = I_2 \otimes I_2 \otimes Z$, ossia $Z_t|abt\rangle = (-1)^t|abt\rangle$. $|0\rangle = (1,0)^T$, $|1\rangle = (0,1)^T$.

Ripristinare l'ausiliario conservando la fase sui dati

Ripartiamo da $|\Psi_2\rangle = (|000\rangle + |010\rangle + |100\rangle - |111\rangle)/2$. Applichiamo di nuovo Toffoli: la porta conserva i coefficienti e riporta il terzo bit a zero in ogni termine.



$$|\Psi_3\rangle \;=\; T|\Psi_2\rangle$$

$$T\frac{|000\rangle}{2} = \frac{|000\rangle}{2}, \quad T\frac{|010\rangle}{2} = \frac{|010\rangle}{2},$$
$$T\frac{|100\rangle}{2} = \frac{|100\rangle}{2}, \quad T\frac{-|111\rangle}{2} = -\frac{T|111\rangle}{2} = -\frac{|110\rangle}{2}.$$
$$|\Psi_3\rangle = \frac{|000\rangle + |010\rangle + |100\rangle - |110\rangle}{2}.$$

Il segno resta sul contributo con $a = b = 1$; il bersaglio è tornato a zero.

Sequenza: T, poi Z_t, poi T.

$$|\Psi_3\rangle = \frac{|00\rangle \otimes |0\rangle + |01\rangle \otimes |0\rangle + |10\rangle \otimes |0\rangle - |11\rangle \otimes |0\rangle}{2} = \frac{|00\rangle + |01\rangle + |10\rangle - |11\rangle}{2} \otimes |0\rangle.$$

Il bersaglio è tornato a zero e si fattorizza dai dati. Ripetiamo la sequenza con pesi numerici differenti per seguire ogni operazione.

$T|a,b,t\rangle = |a,b,t \oplus ab\rangle$; $a,b,t \in \{0,1\}$. $\oplus$: XOR; $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z_t|abt\rangle = (-1)^t|abt\rangle$. $(-1)^{ab} = -1$ soltanto per $a = b = 1$. $|ab,t\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$.

Usare AND per modificare una componente numerica

Riprendiamo l'ingresso già usato per misurare AND: $|\Psi_0\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|110\rangle$, con norma quadrata $9/25 + 16/25 = 1$. Il controllo $b = 1$ e l'ausiliario $t = 0$ isolano i casi inattivo e attivo. Vogliamo assegnare un segno meno al contributo con $a = b = 1$ e recuperare infine l'ausiliario in zero.

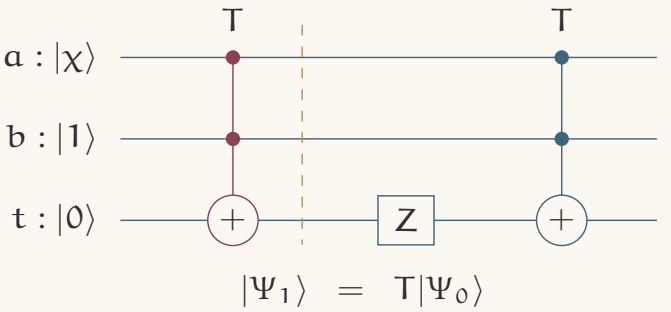
La prima Toffoli calcola il predicato:

$$T|010\rangle = |01, 0 \oplus 0\rangle = |010\rangle,$$

$$T|110\rangle = |11, 0 \oplus 1\rangle = |111\rangle,$$

$$|\Psi_1\rangle = T|\Psi_0\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle.$$

I controlli restano disponibili. Il terzo bit distingue ora il contributo cui deve essere assegnata la fase.



La sequenza prevede Toffoli, Z sul terzo qubit e una seconda Toffoli.

La memoria contiene il valore di AND. Applichiamo Z per moltiplicare per -1 soltanto il termine con terzo indice uguale a uno.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z_t = I_2 \otimes I_2 \otimes Z$. $|\chi\rangle = (3|0\rangle + 4|1\rangle)/5$; $|\Psi_0\rangle = |\chi\rangle|1\rangle|0\rangle$.

Applicare la fase al contributo selezionato

Ripartiamo da $|\Psi_1\rangle = \frac{3}{5}|010\rangle + \frac{4}{5}|111\rangle$. La porta Z_t agisce sul terzo qubit. Svolgiamo i prodotti sui due possibili valori dell'ausiliario:

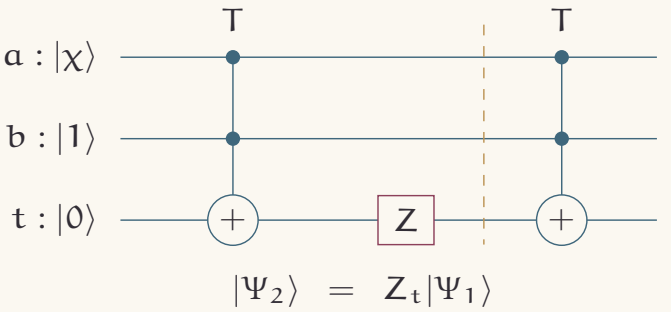
$$Z|0\rangle = \begin{pmatrix} 1\cdot 1 + 0\cdot 0 \\ 0\cdot 1 - 1\cdot 0 \end{pmatrix} = |0\rangle, \qquad Z|1\rangle = \begin{pmatrix} 1\cdot 0 + 0\cdot 1 \\ 0\cdot 0 - 1\cdot 1 \end{pmatrix} = -|1\rangle.$$

Per i due contributi dello stato congiunto,

$$Z_t|010\rangle = |010\rangle, \qquad Z_t|111\rangle = -|111\rangle.$$

Per linearità,

$$|\Psi_2\rangle = Z_t|\Psi_1\rangle = \frac{3}{5}|010\rangle - \frac{4}{5}|111\rangle.$$



Il terzo qubit seleziona il segno.

La norma resta $|3/5|^2 + |-4/5|^2 = 9/25 + 16/25 = 1$. Ripristiniamo l'ausiliario con la seconda Toffoli.

$T|a,b,t\rangle = |a,b,t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0\oplus 0 = 1\oplus 1 = 0$, $0\oplus 1 = 1\oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z_t|abt\rangle = (-1)^t|abt\rangle$; $|\Psi_2\rangle = (3|010\rangle - 4|111\rangle)/5$. $|\chi\rangle = (3|0\rangle + 4|1\rangle)/5$; ingresso $|\chi\rangle|1\rangle|0\rangle$.

Ripristinare la memoria dopo la fase

Ripartiamo da $|\Psi_2\rangle = \frac{3}{5}|010\rangle - \frac{4}{5}|111\rangle$. La seconda Toffoli usa gli stessi due controlli:

$$T|010\rangle = |01, 0 \oplus (0 \cdot 1)\rangle = |010\rangle, \qquad T|111\rangle = |11, 1 \oplus (1 \cdot 1)\rangle = |110\rangle.$$

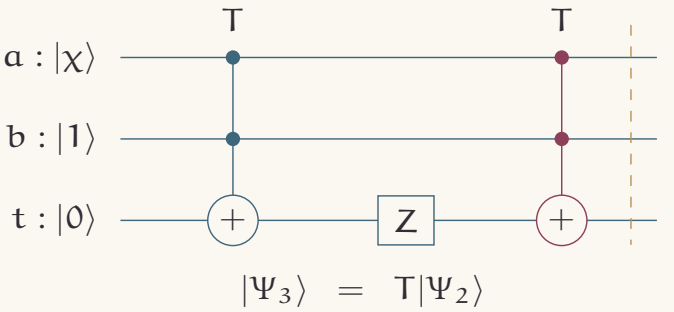
La linearità conserva il coefficiente negativo:

$$|\Psi_3\rangle = T|\Psi_2\rangle = \frac{3}{5}T|010\rangle - \frac{4}{5}T|111\rangle = \frac{3}{5}|010\rangle - \frac{4}{5}|110\rangle.$$

Raccogliamo il terzo fattore, uguale nei due termini:

$$|\Psi_3\rangle = \frac{3}{5}|01\rangle|0\rangle - \frac{4}{5}|11\rangle|0\rangle = \left(\frac{3}{5}|01\rangle - \frac{4}{5}|11\rangle\right) \otimes |0\rangle.$$

L'ausiliario torna separato dai dati e può essere riutilizzato.



Il segno relativo rimane nei dati dopo il ripristino della memoria.

La norma finale vale $9/25 + 16/25 = 1$. I dati conservano i pesi iniziali, mentre lo stato contiene la fase introdotta.

$T|a, b, t\rangle = |a, b, t \oplus ab\rangle$; a, b: controlli, t: ausiliario. $\oplus$: XOR, $0 \oplus 0 = 1 \oplus 1 = 0$, $0 \oplus 1 = 1 \oplus 0 = 1$. Base $(000, 001, 010, 011, 100, 101, 110, 111)$; $|abt\rangle = |a\rangle \otimes |b\rangle \otimes |t\rangle$. $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$; $Z_t|abt\rangle = (-1)^t|abt\rangle$; $|\Psi_2\rangle = (3|010\rangle - 4|111\rangle)/5$. $|\chi\rangle = (3|0\rangle + 4|1\rangle)/5$; ingresso $|\chi\rangle|1\rangle|0\rangle$.

Riferimenti e strumenti del percorso

Il percorso collega porte, interferenza e logica reversibile agli algoritmi di Deutsch e Deutsch–Jozsa. Il riferimento del materiale originale è N. David Mermin, *Quantum Computer Science: An Introduction*, Cambridge University Press, 2007, capitoli 1 e 2.

Per il modello a oracolo e il confronto fra procedure esatte e probabilistiche: IBM Quantum Learning, *Fundamentals of Quantum Algorithms*, lezioni The query model of computation e The Deutsch–Jozsa algorithm.

A. A. Abbott, *The Deutsch–Jozsa Problem: De-quantisation and Entanglement*, Natural Computing 11, 3–11 (2012), arXiv:0910.1990, discute il problema e il significato del confronto fra modelli.

Convenzioni: A precede B nel prodotto tensoriale; x_1 è il primo bit della stringa; la base segue l'ordine lessicografico. n indica il numero di qubit di A, d il bit finale di classificazione.

Le fonti sono state consultate per verificare il modello di accesso, la promessa del problema e l'ambito del vantaggio dimostrato.

A: registro dell'argomento; B: ausiliario. $U_f|x,y\rangle = |x, y \oplus f(x)\rangle$. Per Deutsch, $d = f(0) \oplus f(1)$. Per Deutsch–Jozsa, si misura z e si calcola $d = z_1 \vee \cdots \vee z_n$; $d = 0$ indica la classe costante, $d = 1$ la bilanciata.