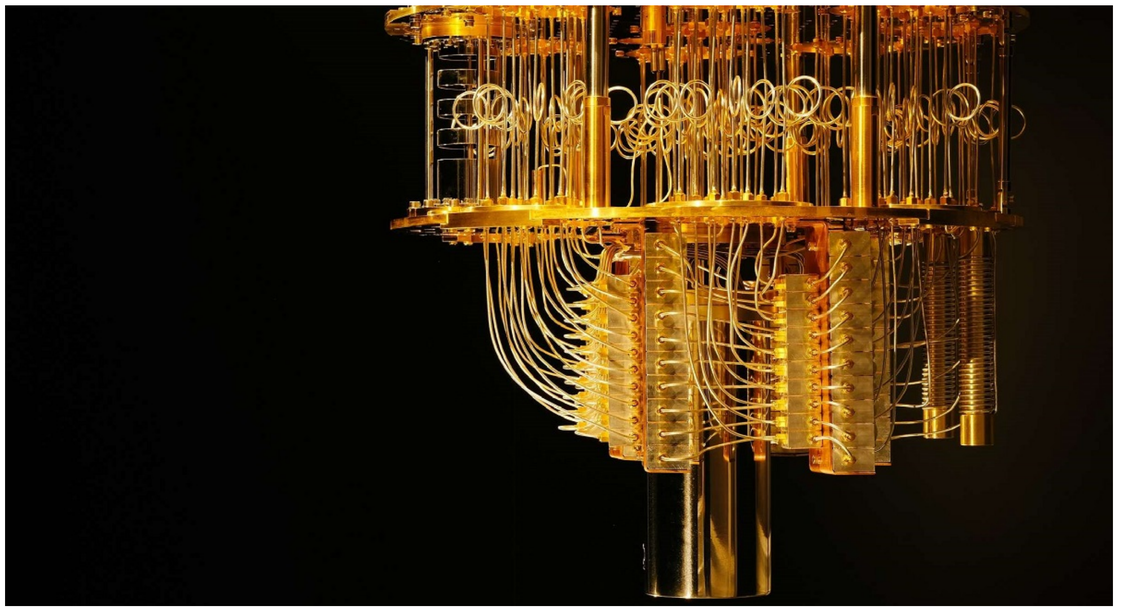
Tecnologie quantistiche

Didattica della fisica quantistica

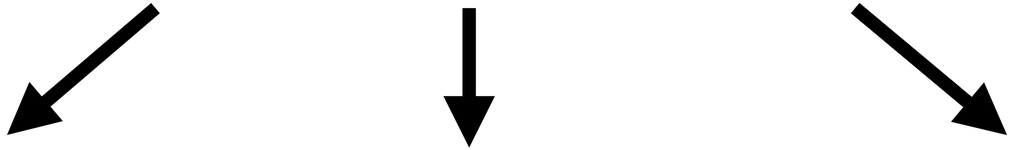


PLS 2020-2021 - Università degli studi di Pavia - Fisica

Chiara Macchiavello
Lidia Falomo
Massimiliano Malgieri
Claudio Sutrini

Percorso

I primi tre incontri



Termodinamica del calcolo
Logica reversibile

FQ dispositivo S&G
Principio di sovrapposizione
Osservabili non compatibili

Dal bit al qubit
C i r c u i t i
quantistici

Strumenti utili

Qubit

$$|0\rangle, \quad |1\rangle$$

$$|0\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad |1\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Prodotto scalare

$$|\phi\rangle \cdot |\psi\rangle = \langle\phi|\psi\rangle = \sum_{i=0}^{1} \phi_i^* \psi_i$$ con ϕ^* complesso coniugato

$$|\phi\rangle \cdot |\psi\rangle = \langle\phi|\psi\rangle = [\phi_0^*, \phi_1^*] \begin{bmatrix} \psi_0 \\ \psi_1 \end{bmatrix} = \phi_0^* \psi_0 + \phi_1^* \psi_1$$

Postulati prodotto scalare:

1. $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$
2. $\langle\psi|a\phi + b\chi\rangle = a\langle\psi|\phi\rangle + b\langle\psi|\chi\rangle$
3. $\langle\psi|\psi\rangle \geq 0$

Base

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

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

$$\alpha, \beta \in C$$

$$|\psi\rangle = \alpha \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \beta \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$$

$$|\alpha|^2 = |\langle 0|\psi\rangle|^2 = P_0 \quad |\beta|^2 = |\langle 1|\psi\rangle|^2 = P_1$$ (o)

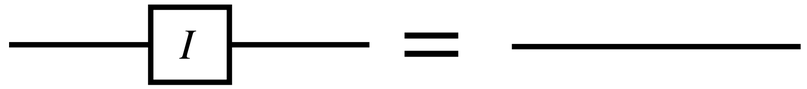
P_0, P_1 sono rispettivamente la probabilità di far collassare lo stato $|\psi\rangle$ in $|0\rangle$ e in $|1\rangle$ (valori ± 1 della misura).

Strumenti utili

Identità:

$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$\|1\rangle$

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad |\psi\rangle \longmapsto |\psi\rangle$$



Not (X):

$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|1\rangle + \beta|0\rangle$$

Hadamard

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

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad \alpha|0\rangle + \beta|1\rangle \longmapsto \alpha|+\rangle + \beta|-\rangle$$

Phase flip (Z):

$\|0\rangle$	$\|0\rangle$
$\|1\rangle$	$-\|1\rangle$

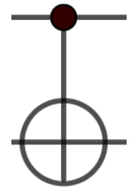
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \qquad \alpha|0\rangle \pm \beta|1\rangle \longmapsto \alpha|0\rangle \mp \beta|1\rangle$$

$$|+\rangle \xmapsto{Z} |-\rangle$$
$$|-\rangle \xmapsto{Z} |+\rangle$$

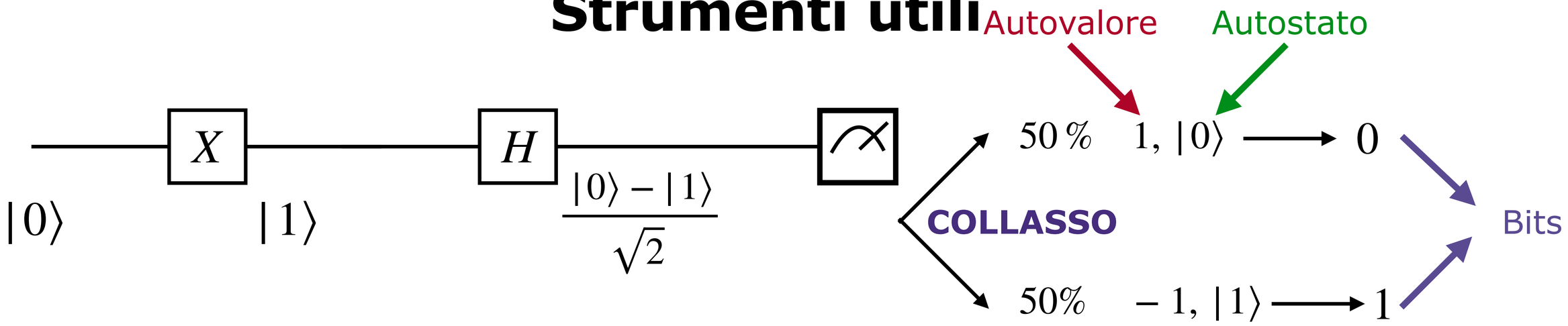
CNOT:

$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad |x\rangle|y\rangle \longmapsto |x\rangle|x \oplus y\rangle$$



Strumenti utili



$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} \xrightarrow{X} \begin{bmatrix} 0 \\ 1 \end{bmatrix} \xrightarrow{H} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} := |\psi\rangle$$

$$|\langle 0|\psi\rangle|^2 = 0.5$$

$$|\langle 1|\psi\rangle|^2 = 0.5$$

$$X \quad \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$$H \quad \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$P_0 = |\langle 0|\psi\rangle|^2 = \left| [1,0] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right|^2 = 0.5$$

$$P_1 = |\langle 1|\psi\rangle|^2 = \left| [0,1] \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} \right|^2 = 0.5$$

Strumenti utili

In generale il prodotto tensore tra due qubit

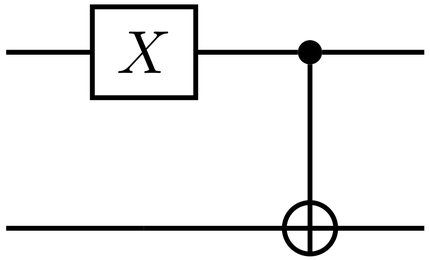
$$|\psi\rangle \otimes |\phi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \otimes \begin{bmatrix} \gamma \\ \delta \end{bmatrix} = \begin{bmatrix} \alpha \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \\ \\ \beta \begin{bmatrix} \gamma \\ \delta \end{bmatrix} \end{bmatrix}$$

Analogamente tra due operatori $A \otimes B$.
Per esempio:

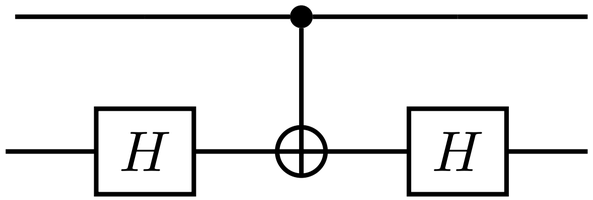
$$X \otimes H = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \begin{bmatrix} 0 \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & 1 \cdot \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\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

Esempi ed esercizi: correzione

1)

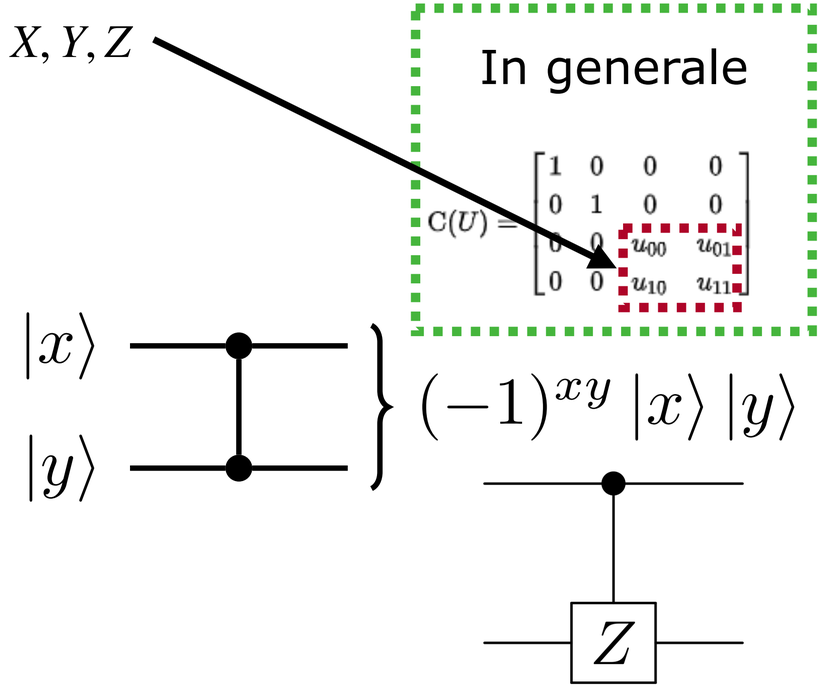


2)

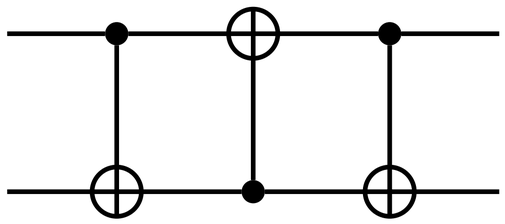


IN		OUT
$\|00\rangle$	$\rightarrow$	$\|00\rangle$
$\|01\rangle$	$\rightarrow$	$\|01\rangle$
$\|10\rangle$	$\rightarrow$	$\|10\rangle$
$\|11\rangle$	$\rightarrow$	$-\|11\rangle$

C-Z gate



3)



$$|x\rangle\,|y\rangle \longmapsto |x\rangle\,|x \oplus y\rangle$$

Che cosa fa il seguente circuito?

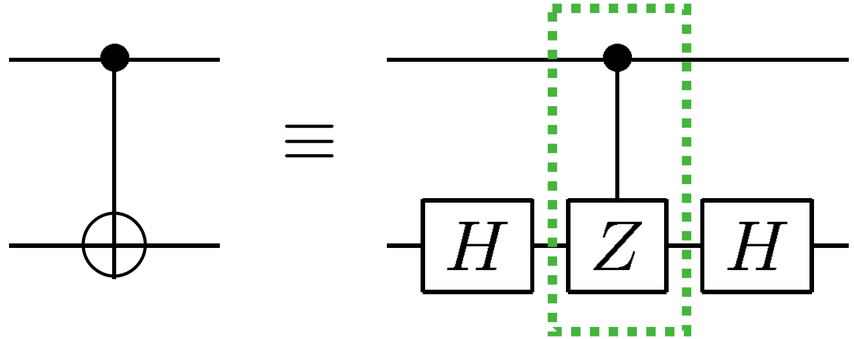
Di quale porta logica classica è il corrispettivo?

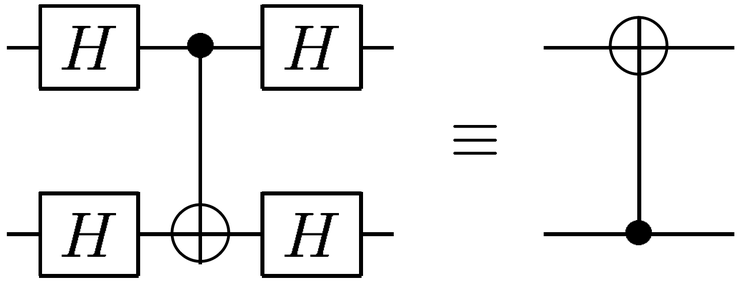
Senza svolgere calcoli, come sarà la sua matrice?

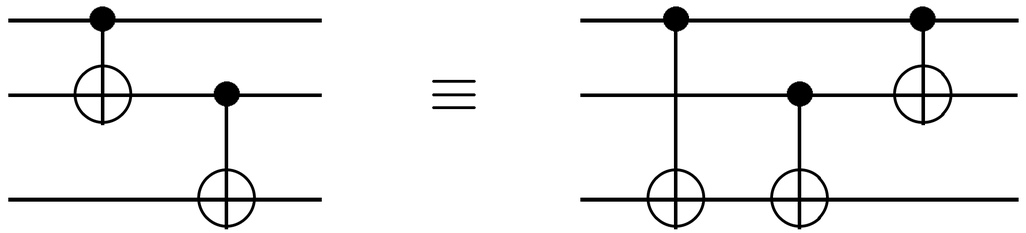
$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Esempi ed esercizi: correzione

4) Dimostrare l’equivalenza dei seguenti circuiti





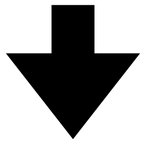


Algoritmi quantistici

Abbiamo visto che gli elementi fondamentali del computer classici sono funzioni booleane del tipo

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

Un computer può implementare ogni funzione assemblando queste funzioni booleane

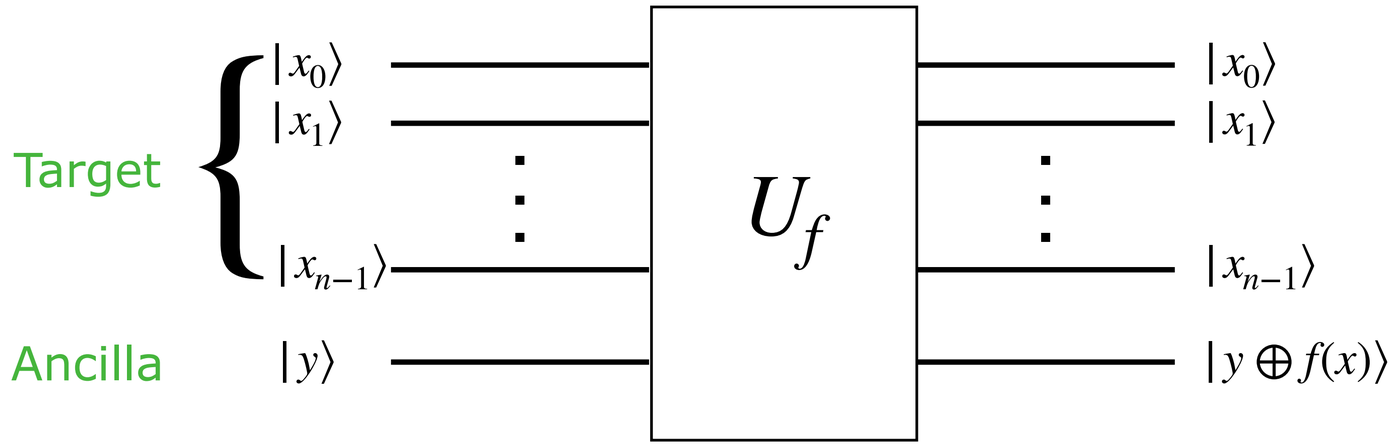


Domanda: possiamo implementare questo tipo di funzioni su un computer quantistico?

Algoritmi quantistici

Risposta: in realtà conosciamo già la risposta! Gli operatori quantistici sono invertibili. Allora si tratta di aggiungere bit (qubit) ausiliari (ancilla).

$$|x_0 x_1 \dots x_{n-1}\rangle\,|y\rangle \longmapsto |x_0 x_1 \dots x_{n-1}\rangle\,|y \oplus f(x_0 x_1 \dots x_{n-1})\rangle = |x_0 x_1 \dots x_{n-1}\rangle\,|y \oplus f(x)\rangle$$

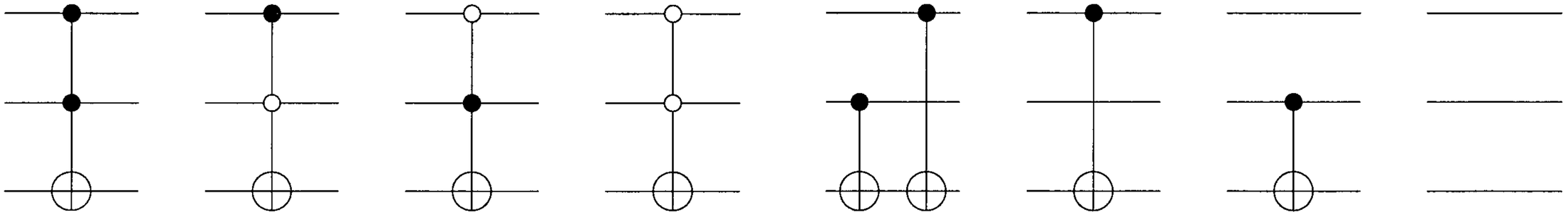


Algoritmi quantistici

Nel caso particolare in cui $n = 2$, l'insieme delle funzioni booleane è rappresentato nella seguente tabella in cui possiamo individuare alcune delle tavole di verità note:

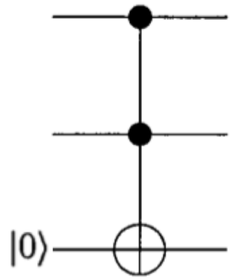
$x_1 x_0$	f_0	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}
0 0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0 1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
1 0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
1 1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Si potrebbe dimostrare (**Esercizio**) che per ottenere tutte le funzioni si possono utilizzare le porte logiche:

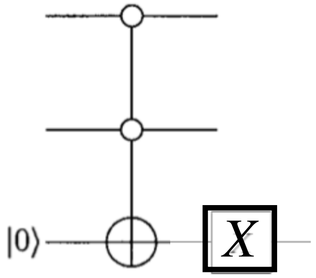


Algoritmi quantistici

Esercizio: dimostrare che la porta logica AND si implementa tramite il seguente circuito



Esercizio: dimostrare che la porta logica OR si implementa tramite il seguente circuito

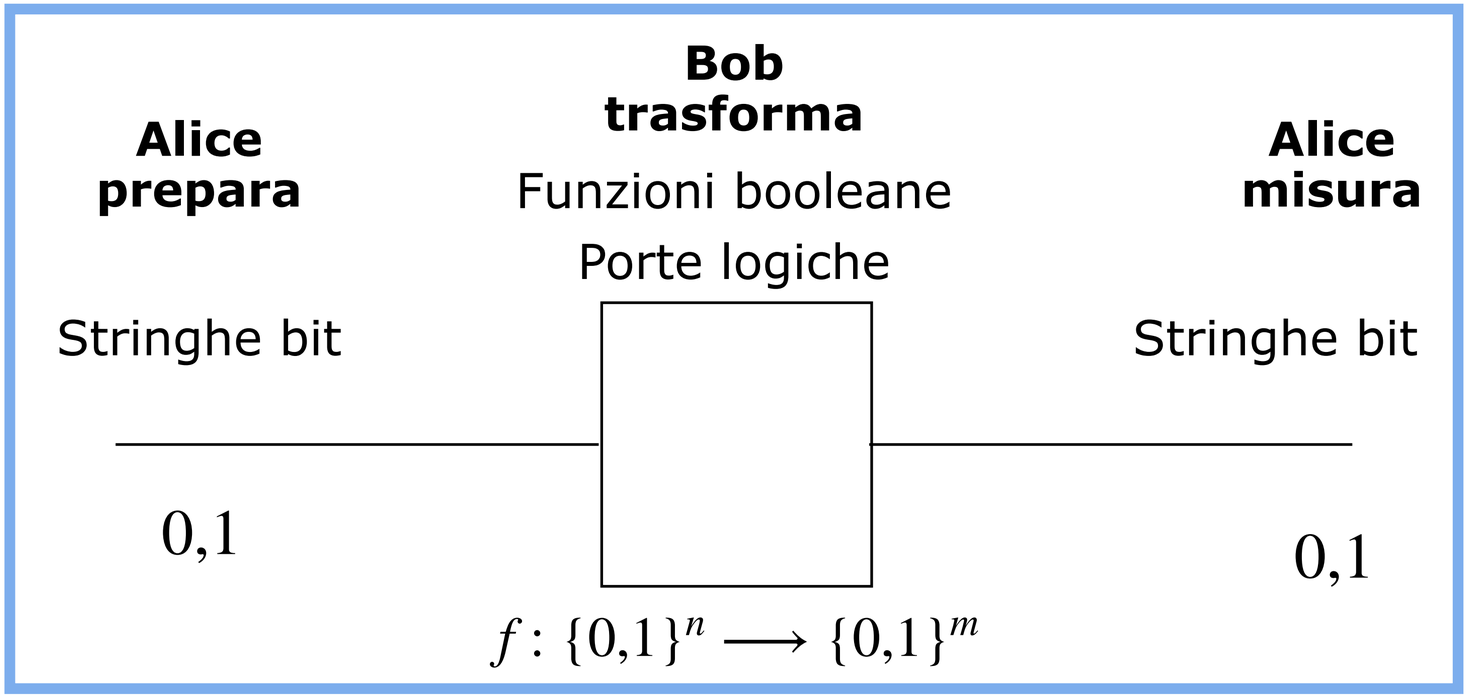


Algoritmo di Deutsch

Alice, da Amsterdam, seleziona un numero x *da* 0 *a* $2^n - 1$*, e lo manda in una lettera a Bob che vive a Boston. Bob inserisce questo numero in una funzione* $f(x)$ *e risponde con una lettera contenente il risultato che può essere solo* 0 *oppure* 1*. Bob ha promesso di usare questa funzione che può agire solo in uno di questi due modi: o* $f(x)$ *è costante per ogni valore di* x*, oppure è bilanciata, ossia è uguale a* 1 *per esattamente metà dei possibili* x *e* 0 *per la rimanente metà. L'obiettivo di Alice è quello di determinare con certezza se Bob ha scelto la funzione costante o bilanciata spedendosi meno lettere possibile. Quanto rapidamente Alice potrà stabilire che funzione sta utilizzando Bob?*

Algoritmo di Deutsch

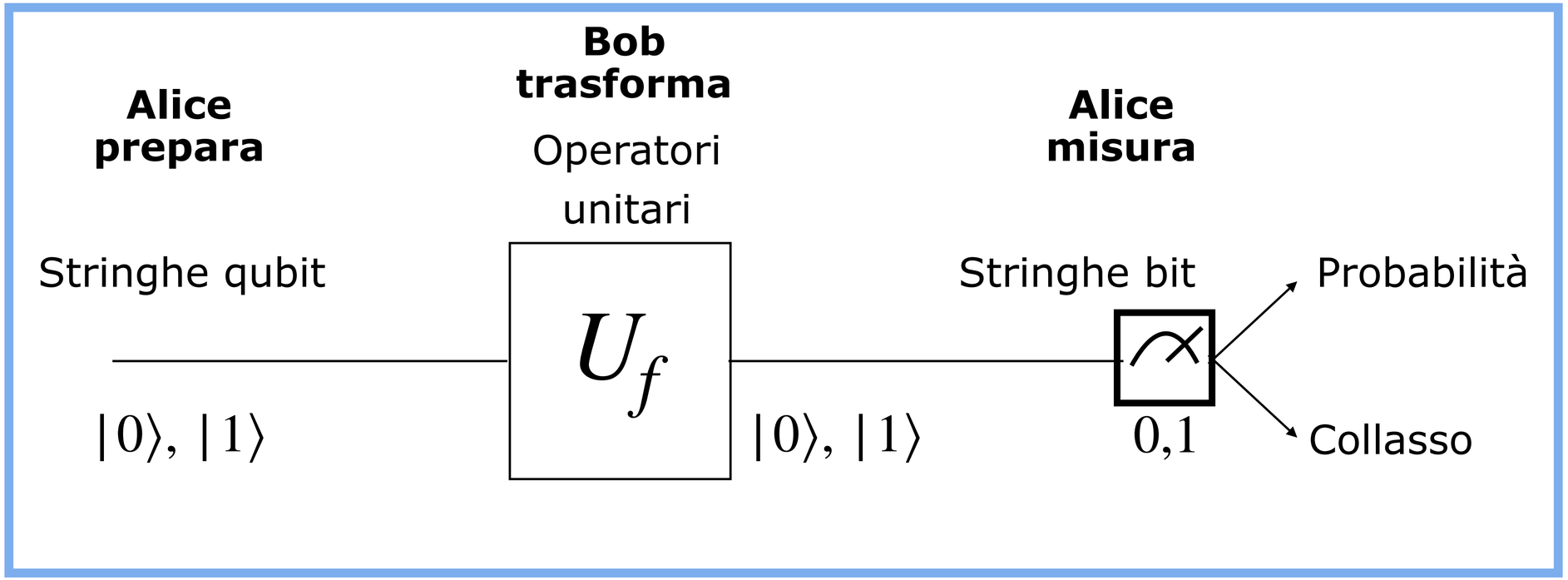
SOLUZIONE CLASSICA



CLASSICAMENTE: Alice ha bisogno che Bob, nel caso peggiore, implementi la propria funzione $\frac{2^n}{2} + 1$ volte prima che Alice possa rispondere con certezza.

Algoritmo di Deutsch

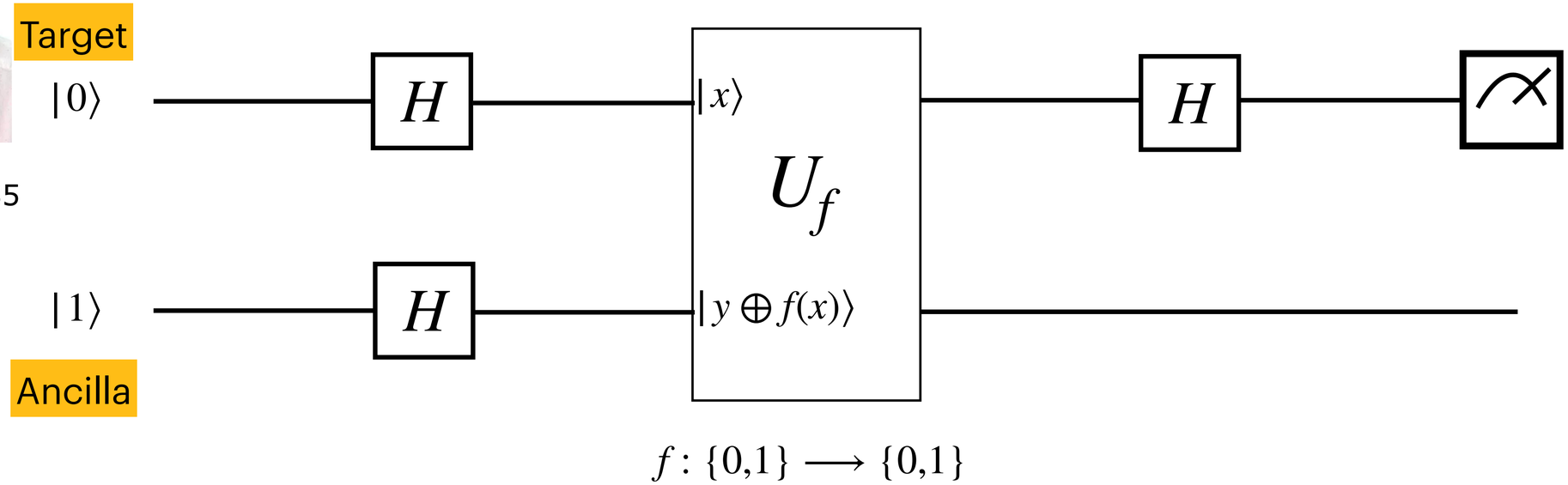
IMPOSTAZIONE QUANTISTICA



Vediamo come possiamo sfruttare la computazione quantistica per rendere molto più efficiente la soluzione.

Algoritmo di Deutsch

David Deutsch, 1985

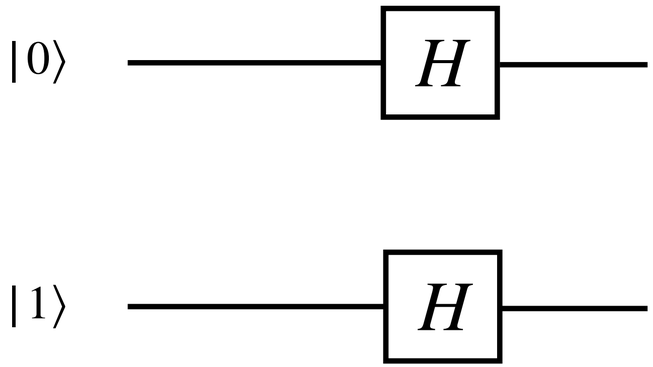


$f : \{0,1\} \longrightarrow \{0,1\}$

Abbiamo tutti gli elementi per analizzare il circuito da un punto di vista formale e concettuale

Algoritmo di Deutsch

Alice prepara



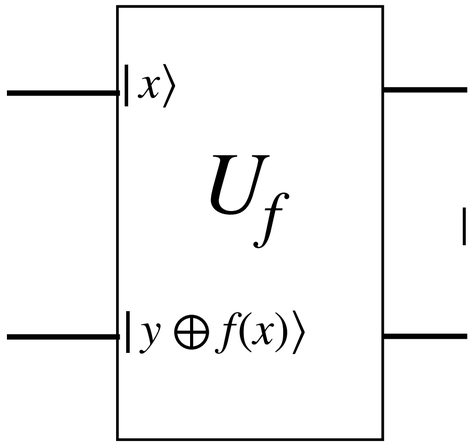
Alice prepara un *qubit* in stato di sovrapposizione per avere in un unico stato codificati entrambi i numeri “numero 0” e “numero 1”

utilizza un *qubit ausiliario* che ha la funzione di creare interferenza

$$|\psi_0\rangle = \left[\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\right] = \frac{1}{2}[|00\rangle - |01\rangle + |10\rangle - |11\rangle]$$

Algoritmo di Deutsch

Bob trasforma



Vediamo ora come agisce l'oracolo (Black box)

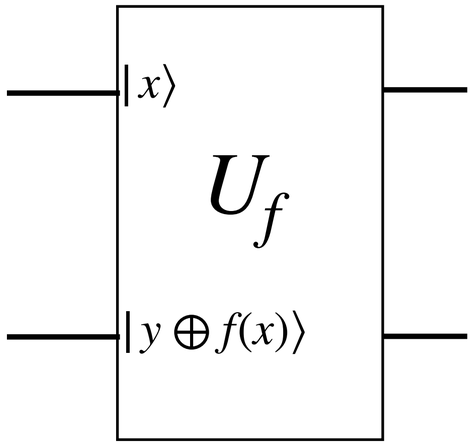
$$|\psi_0\rangle = \frac{1}{2}[|00\rangle - |01\rangle + |10\rangle - |11\rangle] \longmapsto \frac{1}{2}[|0,0 \oplus f(0)\rangle - |0,1 \oplus f(0)\rangle + |1,0 \oplus f(1)\rangle - |1,1 \oplus f(1)\rangle]$$

Possiamo ora affrontare i calcoli successivi in due modi:

1. fare i conti espliciti per tutte le quattro funzioni f possibili
2. mostrare cosa accade se f è bilanciata o costante

Algoritmo di Deutsch

Bob trasforma



Calcoli espliciti

$$|\psi_1\rangle = \frac{1}{2}[\,|0,0 \oplus f(0)\rangle - |0,1 \oplus f(0)\rangle + |1,0 \oplus f(1)\rangle - |1,1 \oplus f(1)\rangle]$$

1. $f(0) = f(1) = 0$
2. $f(0) = f(1) = 1$
3. $f(0) = 0 \ \wedge \ f(1) = 1$
4. $f(0) = 1 \ \wedge \ f(1) = 0$

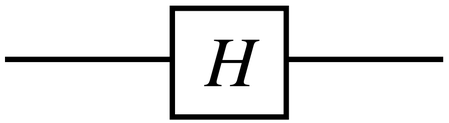
Esempio

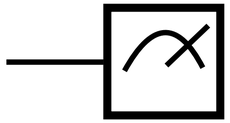
2. $f(0) = f(1) = 1$ $\quad \frac{1}{2}[\,|0,0 \oplus f(0)\rangle - |0,1 \oplus f(0)\rangle + |1,0 \oplus f(1)\rangle - |1,1 \oplus f(1)\rangle] = \frac{1}{2}[\,|0,1\rangle - |0,0\rangle + |1,1\rangle - |1,0\rangle]$

$$= \frac{1}{2}[\,|0\rangle \otimes (|1\rangle - |0\rangle) \ + \ |1\rangle \otimes (|1\rangle - |0\rangle)] = -\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Algoritmo di Deutsch

Alice misura





$$|\psi_1\rangle = -\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \xrightarrow{H \otimes I} |\psi_2\rangle = |0\rangle \otimes \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

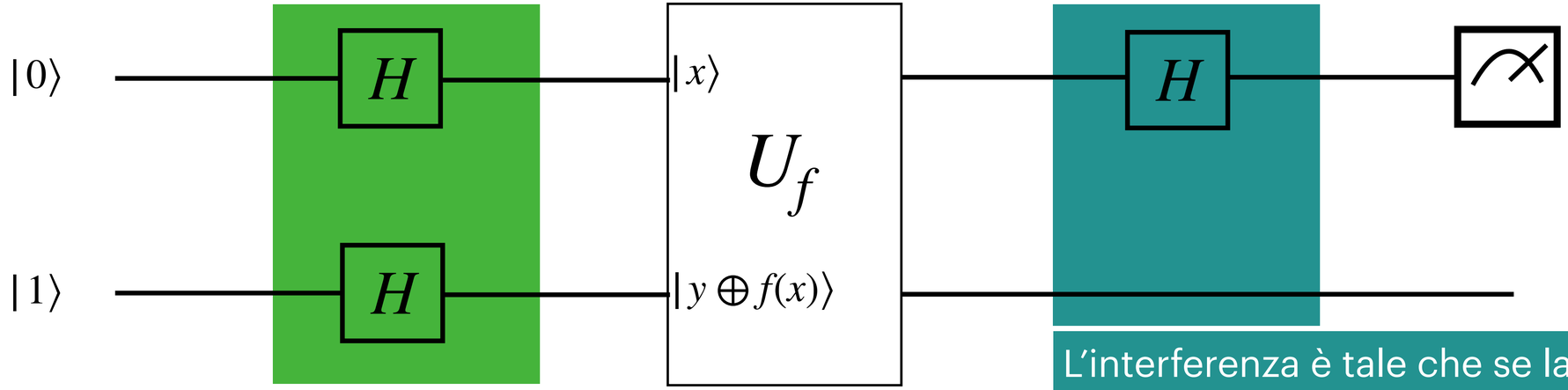
$$P(0) = 1$$

Esercizio: Svolgere i calcoli negli altri 3 casi.

Algoritmo di Deutsch

La porta di Hadamard permette di generare uno stato che risulta sovrapposizione di tutti quelli che codificano le informazioni

N.B. L'operatore U_f ha potuto agire contemporaneamente su tutti gli stati: parallelismo quantistico.



L'interferenza è tale che se la funzione è costante lo stato è trasformato in $|0\rangle$, altrimenti in $|1\rangle$

Si dimostra quindi che se

f è costante → $P(0) = 1$

f è bilanciata → $P(1) = 1$

Abbiamo implementato f UNA SOLA VOLTA!!!

Algoritmo di Deutsch

In generale l'idea è quella di lasciare indisturbato il qubit ancilla e quindi possiamo scrivere[5]

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

da cui tenendo presente che $f(0) = 0, 1$ e $f(1) = 0, 1$ otteniamo

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

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

Algoritmo di Deutsch

A questo punto riapplicando la porta di Hadamard sul primo qubit e l'identità sul secondo otteniamo

$$|\psi_3\rangle = (H \otimes I)\,|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[(-1)^{f(0)}\frac{|0\rangle + |1\rangle}{\sqrt{2}} + (-1)^{f(1)}\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \otimes \frac{|0\rangle - |1\rangle}{\sqrt{2}} =$$

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

A questo punto rimane da fare la misura sullo stato $|\psi_3\rangle$:

1. se la misura dà 1, significa che $f(0) = f(1)$ e risulta che lo stato finale sia
$$|0\rangle = |f(0) \oplus f(1)\rangle$$
2. se la misura dà -1, significa che $f(0) \neq f(1)$ e risulta che lo stato finale sia
$$|1\rangle = |f(0) \oplus f(1)\rangle$$

Algoritmo di Deutsch

CALCOLO MATRICIALE

Accenniamo solamente a come impostare il problema da un punto di vista matriciale

Come abbiamo già visto lo stato iniziale risulta $|0\rangle \otimes |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}$

Su di esso deve agire la matrice $H \otimes H = \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$

La funzione f, a seconda del modo con cui agisce, determina quattro diverse matrici che corrispondono agli operatori lineari che agiscono sui due livelli dell'algoritmo.

Algoritmo di Deutsch

CALCOLO MATRICIALE

- se $f(x) = x$, ossia se f è l'identità I ($f(0) = 0$ e $f(1) = 1$) allora l'operatore U_I agisce nel seguente modo

$$U_I : |x, y\rangle \longmapsto |x, y \oplus f(x)\rangle = |x, y \oplus x\rangle$$

L'operatore U_I dunque modifica il secondo qubit solo se il primo è 1, ossia è una $CNOT - gate$. Con semplici calcoli[7] si può ottenere la matrice associata

$$U_I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Algoritmo di Deutsch

CALCOLO MATRICIALE

- se $f(x) = \overline{x}$, ossia se f è la negazione ($f(0) = 1$ e $f(1) = 0$), allora l'operatore U_X agisce nel seguente modo

$$U_X : |x, y\rangle \longmapsto |x, y \oplus f(x)\rangle = |x, y \oplus (x \oplus 1)\rangle$$

  L'operatore U_X dunque modifica il secondo qubit solo se il primo è zero, ossia è una $Z - CNOT - gate$. La matrice associata risulta

$$U_X = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

- se $f(x) = 0$, ossia se f è sempre vera, allora l'operatore U_T (T=true) agisce nel seguente modo

$$U_T : |x, y\rangle \longmapsto |x, y \oplus f(x)\rangle = |x, y \oplus 0\rangle = |x, y\rangle$$

  L'operatore U_T dunque non modifica il secondo qubit indipendentemente dal valore del primo. La matrice associata risulta

$$U_T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Algoritmo di Deutsch

CALCOLO MATRICIALE

- se $f(x) = 1$, ossia se f è sempre falsa, allora l'operatore U_F (F=False) agisce nel seguente modo

$$U_F : |x, y\rangle \longmapsto |x, y \oplus f(x)\rangle = |x, y \oplus 1\rangle = |x, \overline{y}\rangle$$

  L'operatore U_F dunque modifica il secondo qubit indipendentemente dal valore del primo. La matrice associata risulta

$$U_F = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

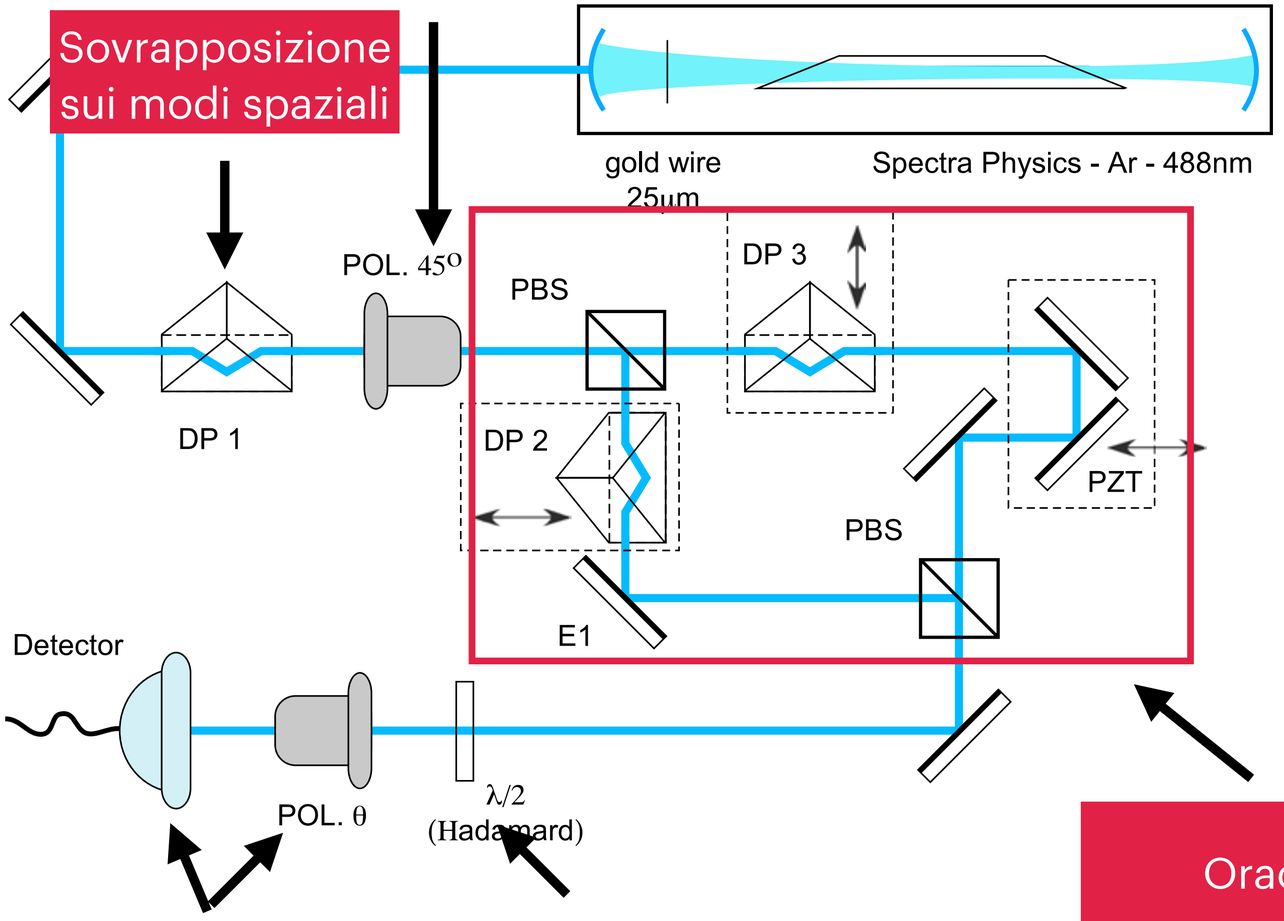
Esercizio: Risolvere l'algoritmo di Deutsch con il linguaggio matriciale nello stesso caso visto in notazione di Dirac.

Algoritmo di Deutsch

REALIZZAZIONE SPERIMENTALE

Sovrapposizione sulla polarizzazione

Sovrapposizione sui modi spaziali



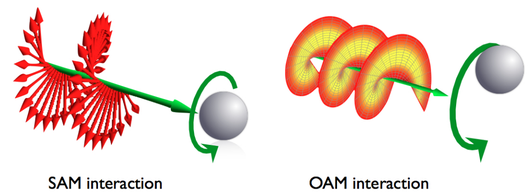
Oracolo

Permettono di verificare che una delle due polarizzazioni ha P=1 e l'altra ha P=0

Interferenza polarizzazione

In questo setup sperimentale i due qubit vengono codificati sfruttando due proprietà della luce: **polarizzazione** e **momento angolare orbitale** (modi spaziali)

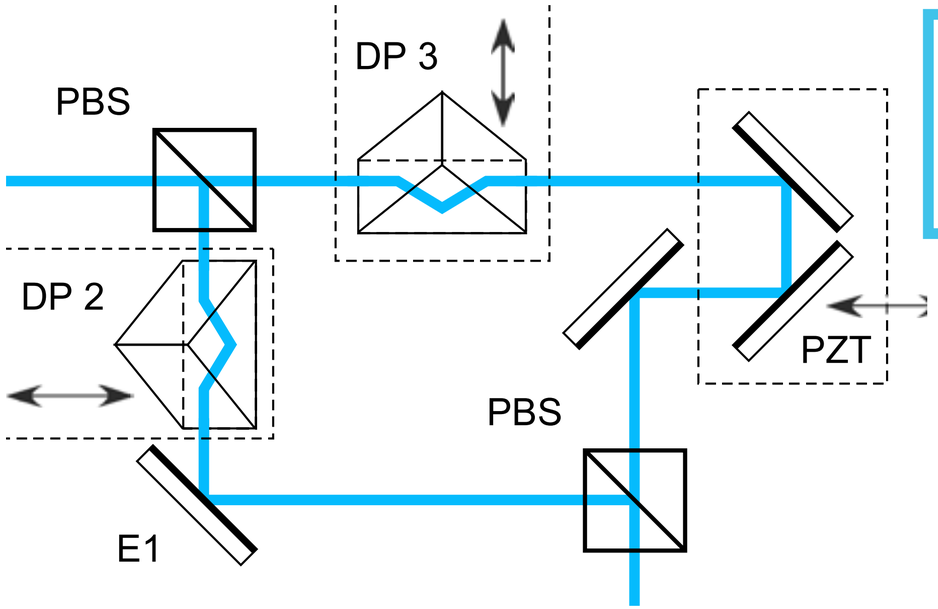
polarization	spatial mode		computational basis
$\|\leftrightarrow\rangle$,	$\|\bullet\bullet\rangle$	$\rightarrow$	$\|0\rangle$
$\|\updownarrow\rangle$,	$\|\bullet\bullet\rangle$	$\rightarrow$	$\|1\rangle$.



Fascio di luce trasporta momento angolare: quando interagisce con una particella di materia essa comincia a ruotare. La rotazione rispetto al proprio asse dipende dal momento angolare di spin (dipende dalla polarizzazione); la rotazione rispetto all'asse del fascio dipende dal momento angolare orbitale (dipende dalla distribuzione spaziale e non dalla polarizzazione)

Algoritmo di Deutsch

REALIZZAZIONE SPERIMENTALE



	Label	Function	Operation
Case 1:	U_{f00}	$f(x) = 0$	$\|x, y\rangle \longrightarrow \|x, y \oplus 0\rangle$
Case 2:	U_{f01}	$f(x) = x$	$\|x, y\rangle \longrightarrow \|x, y \oplus x\rangle$
Case 3:	U_{f10}	$f(x) = \text{inv}(x)$	$\|x, y\rangle \longrightarrow \|x, y \oplus x \oplus 1\rangle$
Case 4:	U_{f11}	$f(x) = 1$	$\|x, y\rangle \longrightarrow \|x, y \oplus 1\rangle$

La parte più interessante del setup è sicuramente quella relativa all'implementazione dell'oracolo. La possibilità di inserire o disinserire nell'interferometro uno o entrambi i *Dove-prism* permette di implementare i quattro operatori corrispondenti

U_{f00} nel primo caso non accade nulla; non serve inserire nulla nell'interferometro;

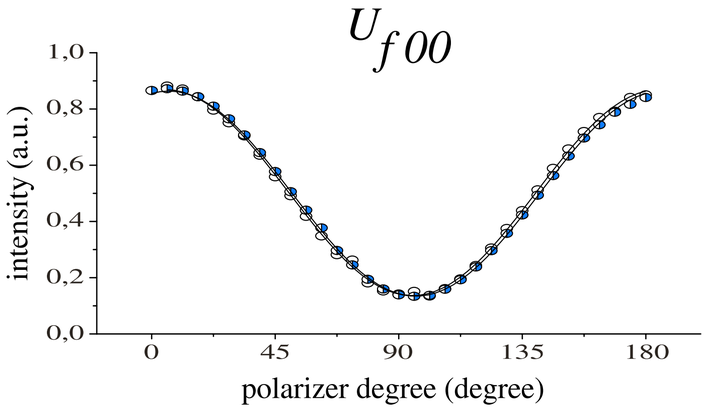
U_{f01} in questo caso siamo in presenza di una *C-NOT gate* che può essere implementata inserendo un dove prism nel braccio dell'interferometro che trasmette luce polarizzata verticalmente: viene modificato il modo spaziale solo se la polarizzazione è verticale;

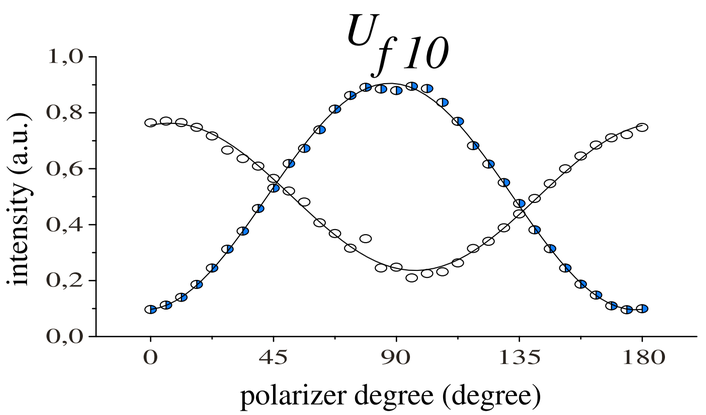
U_{f10} siamo in presenza di una *Z-CNOT gate* che si può ottenere semplicemente spostando il dove prism sull'altro braccio dell'interferometro: viene modificato il modo spaziale solo se la polarizzazione è orizzontale;

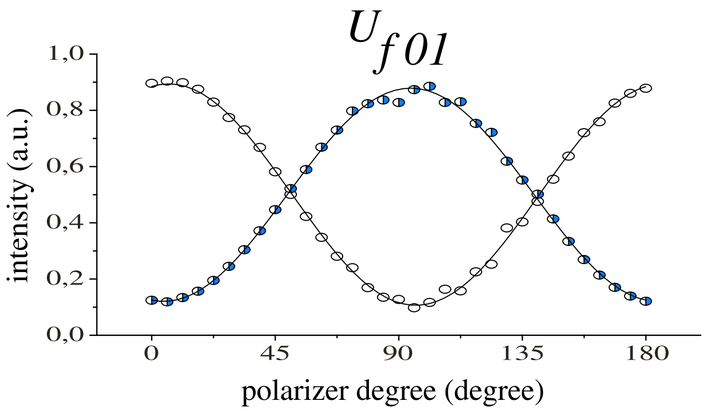
U_{f11} la *NOT gate* si ottiene inserendo due dove prism su entrambi i bracci dell'interferometro: viene modificato il modo spaziale indipendentemente dalla polarizzazione;

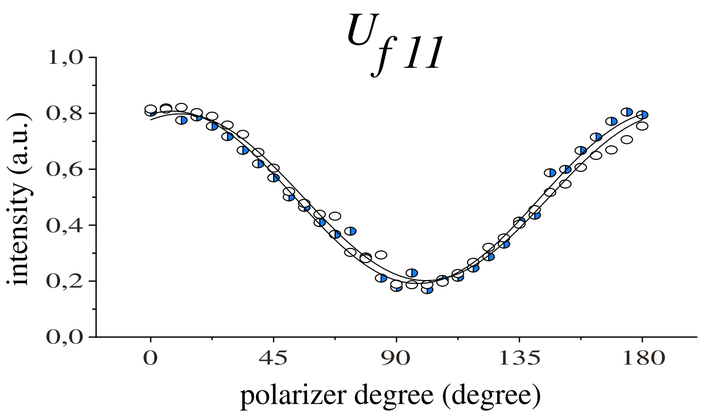
Algoritmo di Deutsch

REALIZZAZIONE SPERIMENTALE



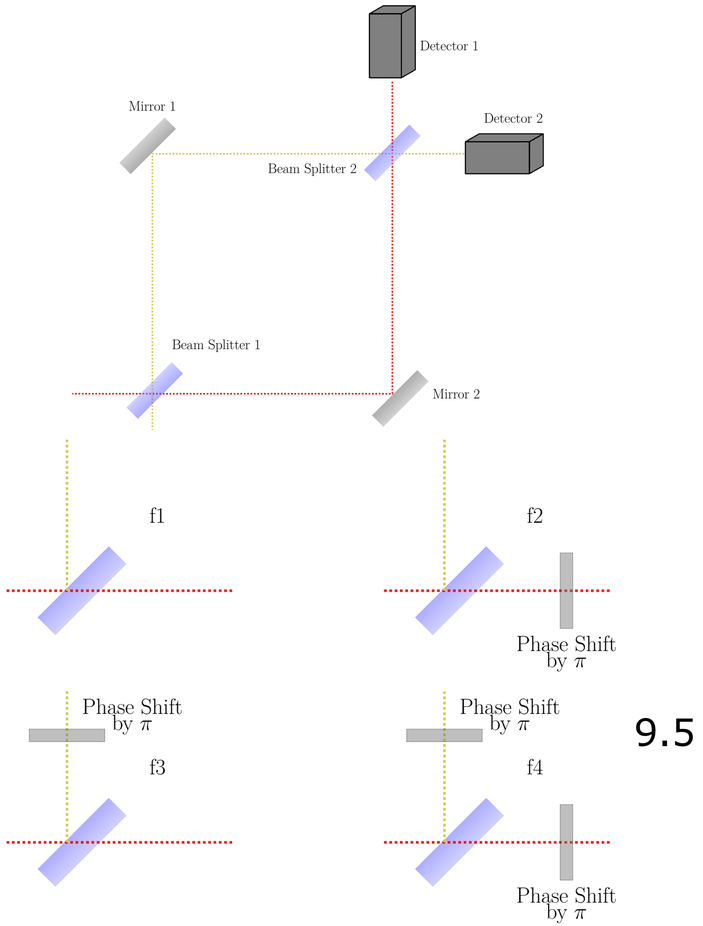






Algoritmo di Deutsch

Interferometro Mach-Zender



9.5

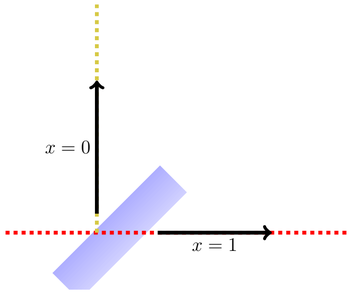
We will not go into the math behind the algorithm, but it can be demonstrated using the Mach-Zehnder interferometer with phase shifters[3] as shown in Figure 9.3. Recall from the chapter on the beam splitter that the beam splitter will shift the phase of a photon depending on whether the photon hits the glass or dielectric side. The π phase shifters are pieces of glass that can be placed along the path to shift the phase an additional 180°. Here is how the algorithm is implemented:

1. The two inputs $x = 0$ and $x = 1$ are represented by the two possible photon paths as shown in Figure 9.4. A photon taking the yellow path is $x = 0$, while a photon taking the red path is $x = 1$. The first beam splitter therefore creates a superposition of 0 and 1 since the photon takes both paths.

2. The four functions will be modeled by four different phase shifter configurations, as shown in Figure 9.5. A phase shifter is placed in the path whenever the function returns a 1.

3. The second beam splitter creates the interference necessary to tell whether there was an odd or even number of phase shifters in the way.

4. Measure which detector is activated. There is only one single measurement made. The single measurement made tells you the answer of the question.



9.4

Algoritmo di Deutsch -Jozsa

Generalizzazione!

RAPINA IN BANCA

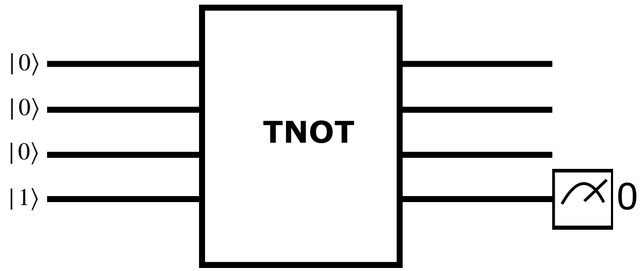
Sei stato assoldato per rapinare una banca celebre per le sue strutture di sicurezza.
La banca è divisa in molti caveaux in ciascuno dei quali ci sono 8 enormi lingotti d'oro.

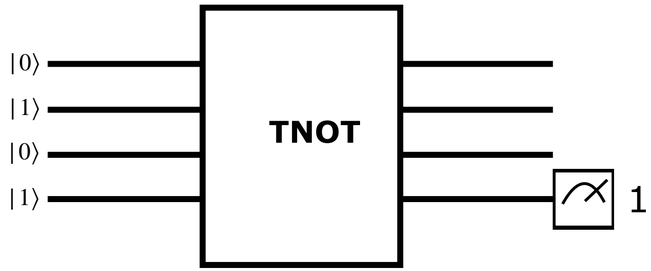
Il capo della banda è venuto a sapere che in ogni stanza o tutti i lingotti sono falsi o metà sono falsi e metà sono veri. Purtroppo la falsità o l'autenticità dei lingotti può essere verificata con apparecchiature troppo sofisticate da poter essere trasportate durante la rapina.
Anche i dipendenti della banca non possono riconoscerne l'autenticità o meno.
Per evitare che una mappa dei lingotti veri possa essere copiata o rubata, il direttore della banca ha deciso di installare un computer (quantistico) in ogni stanza. Ogni lingotto può essere codificato in modo ovvio con dei qubit

Algoritmo di Deutsch - Jozsa

Generalizzazione!

Il computer ha un programma che funziona in questo modo: l'impiegato inserisce su tre registri i qubit corrispondenti al lingotto scelto e su un quarto un qubit $|1\rangle$; se il lingotto è autentico allora al quarto qubit viene applicato un *NOT* altrimenti no. Quindi se l'impiegato vede 0 sullo schermo del computer sa che il lingotto è vero; altrimenti è falso. I primi tre qubit invece riescono esattamente come sono entrati[1].





[1] Possiamo inventarci una porta logica di nome TNOT-gate, ossia una TRUE-NOT gate.

Algoritmo di Deutsch - Jozsa

Generalizzazione!

Esercizio 1: Prova a costruire un circuito in grado di implementare il programma descritto (almeno in qualche caso particolare).

La banda è venuta a conoscenza del funzionamento del programma, ma c'è un ulteriore problema: per aumentare la sicurezza il computer restituisce il risultato in un'ora. Quindi quando sarai all'interno del caveau potrai utilizzarlo solo una volta prima di poter uscire senza essere catturato. Inoltre il capobanda ha deciso che lascerà vivo chi porterà lingotti autentici e ucciderà chi ne porterà solo falsi perché occupano spazio inutile sul furgone[2].
Sembra che per te ci sia una sola soluzione: inserire i qubit di codifica di un lingotto nel computer; se esce 0 puoi festeggiare e correre a portare i lingotti sul furgone, se viene 1 prendere comunque tutti i lingotti e sperare in bene…

Esercizio 2: Sei in grado di modificare il circuito precedente in modo da migliorare le tue probabilità di conoscere in che tipo di caveau sei entrato[3] e far cambiare idea al capo sul suo terribile piano?

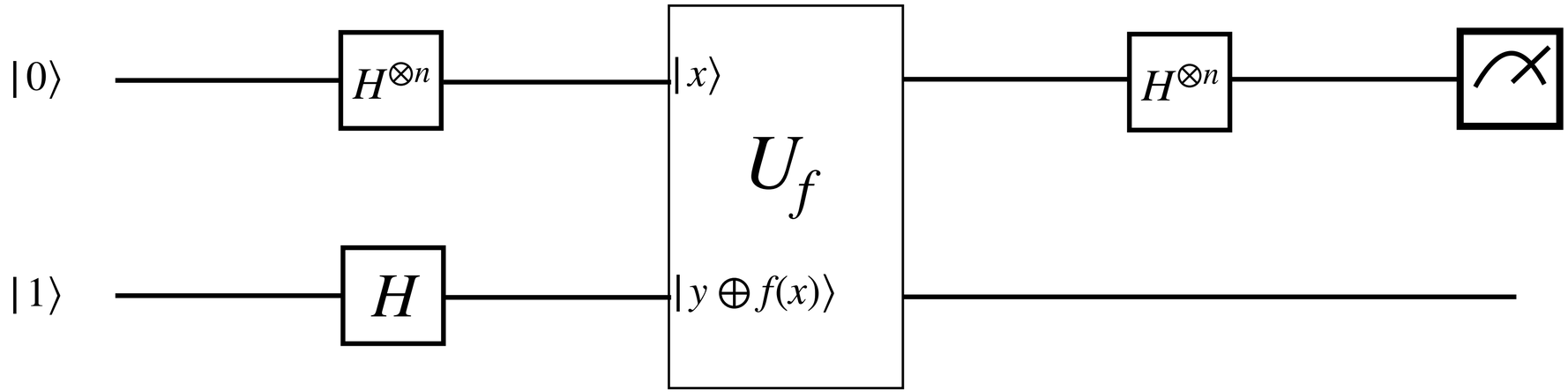
Per semplificare i calcoli puoi provare a trattare prima il caso di 4 lingotti, due veri e due falsi o tutti falsi.

[2] Come ogni capo ha qualche atteggiamento non troppo razionale…

[3] Quello con 8 lingotti falsi o l'altro

Algoritmo di Deutsch-Jozsa

Conclusione



Possiamo implementare f una sola volta grazie alla sovrapposizione e all'interferenza quantistica a differenza del caso classico in cui, nella peggiore delle ipotesi, avremo bisogno di applicarla $\frac{2^n}{2} + 1$ volte.

Algoritmo di ricerca

IMPOSTAZIONE CLASSICA

Gara: 100 m

Antonio
Carlo
Luigi
Stefano

Classifica

1. Luigi
2. Stefano
3. Antonio
4. Carlo

Ricerca: primo classificato

Codifica: 2 bit

Antonio $\longrightarrow (0,0)$
Carlo $\longrightarrow (0,1)$
Luigi $\longrightarrow (1,0)$
Stefano $\longrightarrow (1,1)$

$f : \{0,1\}^2 \longrightarrow \{0,1\}$

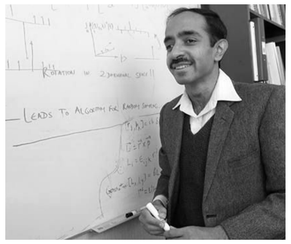
$$(0,0) \longrightarrow 0$$
$$(0,1) \longrightarrow 0$$
$$(1,0) \longrightarrow 1$$
$$(1,1) \longrightarrow 0$$

Ricerca: applico f

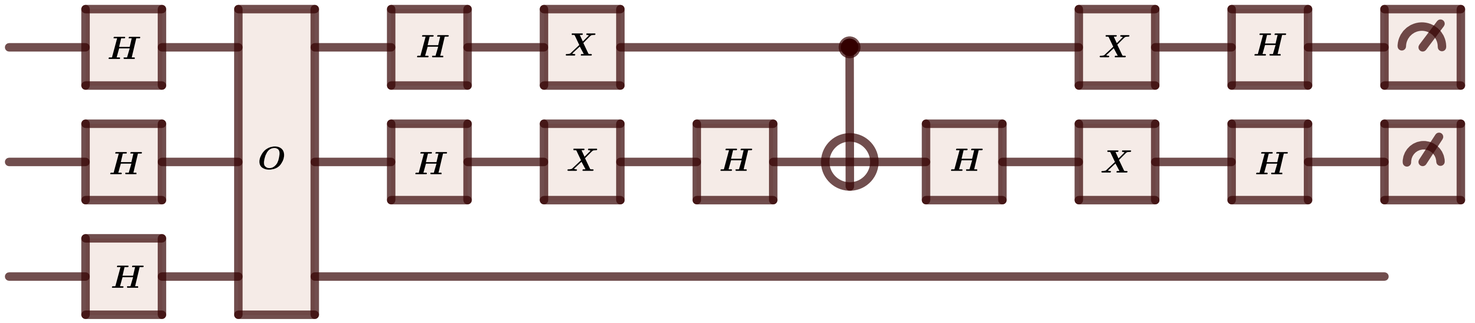
Domanda: quante volte?

Risposta: in media $2^n/2$

Algoritmo di Grover



Lov Grover, 1996



Codifica: 2 bit

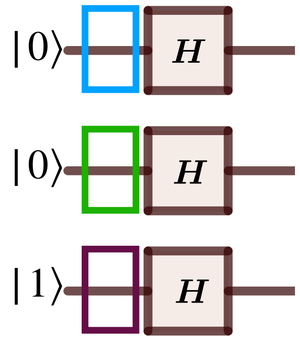
Antonio $\longrightarrow (0,0)$
Carlo $\longrightarrow (0,1)$
Luigi $\longrightarrow (1,0)$
Stefano $\longrightarrow (1,1)$

Codifica: 2 qubit

Antonio $\longrightarrow |0\rangle|0\rangle$
Carlo $\longrightarrow |0\rangle|1\rangle$
Luigi $\longrightarrow |1\rangle|0\rangle$
Stefano $\longrightarrow |1\rangle|1\rangle$

f viene implementata una sola volta

Algoritmo di Grover



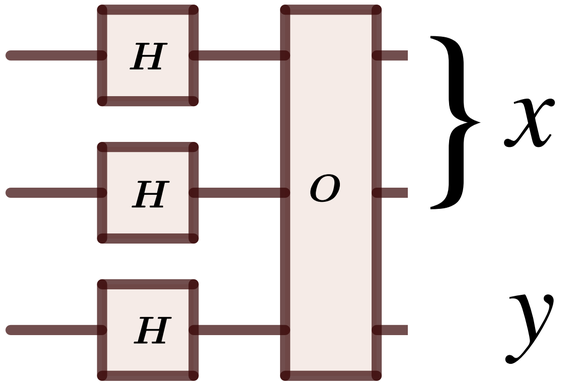
$$|\psi_0\rangle = \left[\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\right]\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) =$$

$$= \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right]\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) =$$

$$= \frac{1}{2\sqrt{2}}\left[|0\rangle|0\rangle|0\rangle - |0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle - |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle - |1\rangle|1\rangle|1\rangle\right]$$

Algoritmo di Grover

$$= \frac{1}{2\sqrt{2}} \left[|0\rangle|0\rangle|0\rangle - |0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|1\rangle + |0\rangle|1\rangle|0\rangle + |1\rangle|0\rangle|0\rangle - |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle - |1\rangle|1\rangle|1\rangle \right]$$



$$|x, y\rangle \longrightarrow |x, y \oplus f(x)\rangle \qquad f(x) = \begin{cases} 1 & se\ x = x_0 \\ 0 & altrimenti \end{cases}$$

$$O(|\psi_0\rangle) = = \frac{1}{2\sqrt{2}} \left[|0\rangle|0\rangle|0\rangle - |0\rangle|0\rangle|1\rangle - |0\rangle|1\rangle|1\rangle + |0\rangle|1\rangle|0\rangle - |1\rangle|0\rangle|0\rangle + |1\rangle|0\rangle|1\rangle + |1\rangle|1\rangle|0\rangle - |1\rangle|1\rangle|1\rangle \right]$$

$$= \left[\frac{1}{2} \left(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle \right) \right] \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) := |\psi_1\rangle$$

N.B. L'operatore O ha potuto agire contemporaneamente su tutti gli stati: parallelismo quantistico.
Agisce quindi una sola volta!

Algoritmo di Grover

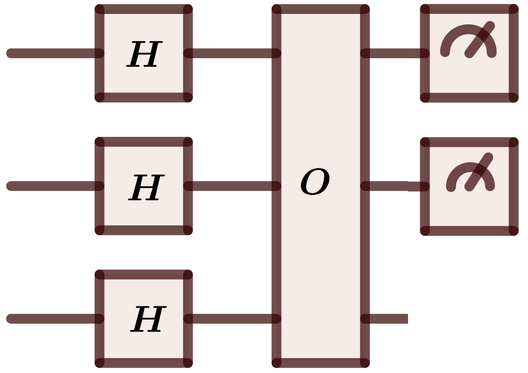
$$|\psi_1\rangle = \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right]\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \qquad |x\rangle \longrightarrow (-1)^{f(x)}|x\rangle$$

L'oracolo ha marchiato con cambiamento di fase sul target la soluzione!

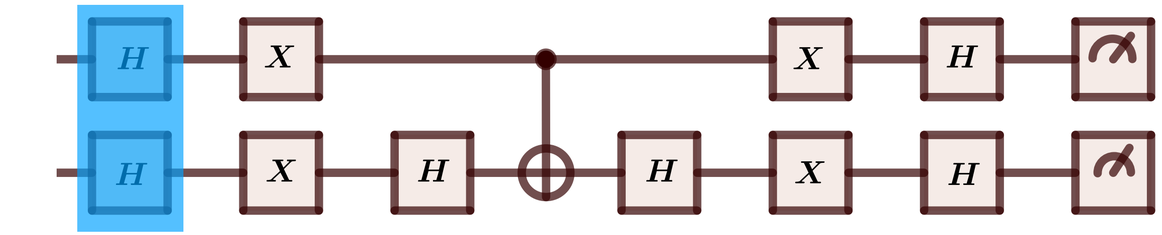
Domanda: abbiamo risolto il problema?

NO!!!

$$P(0,0) = P(0,1) = P(1,0) = P(1,1)$$

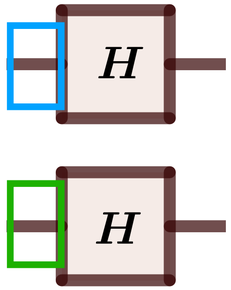


Algoritmo di Grover



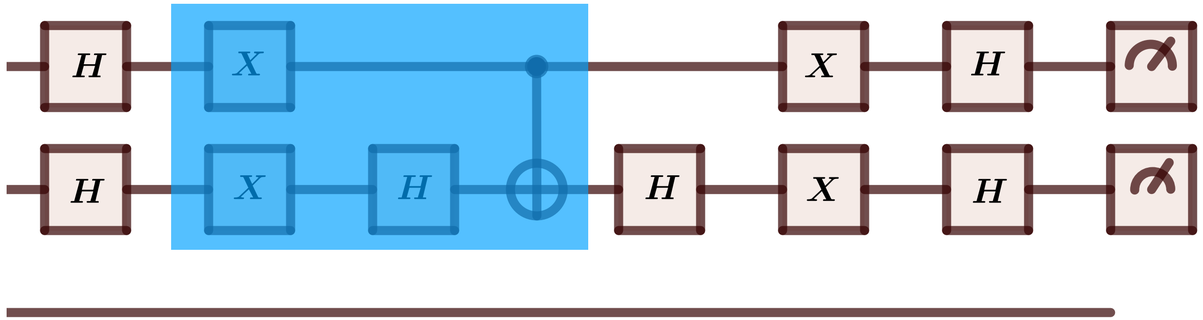
Da questo momento in poi possiamo non considerare l'ultimo registro

$$|\psi_1\rangle = \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right] = \frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right]$$



$$\frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |1\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right] \xrightarrow{H\otimes H} \frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle - \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|1\rangle\right]$$

Algoritmo di Grover

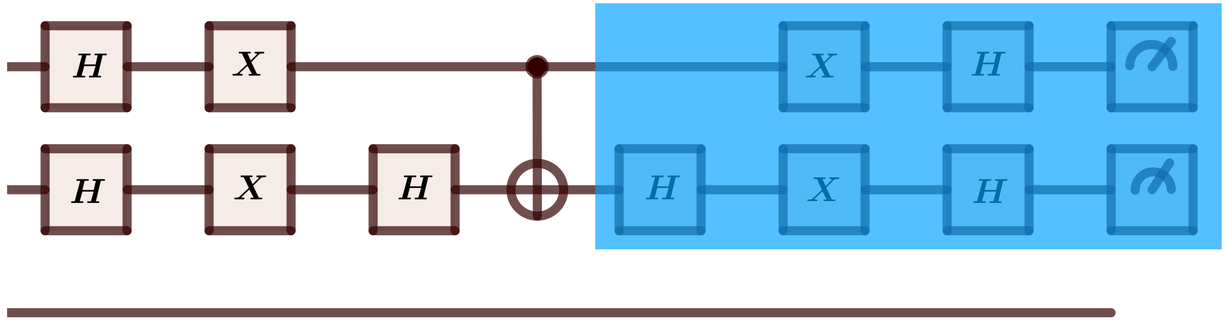


$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|0\rangle - \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|1\rangle\right] \xrightarrow{X\otimes X} \frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|1\rangle + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|0\rangle\right]$$

$$\frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)|1\rangle + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)|0\rangle\right] \xrightarrow{I\otimes H} \frac{1}{\sqrt{2}}\left[\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) + \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right] =$$

$$= \ldots = \frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |1\rangle|1\rangle] \xrightarrow{CNOT} \frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |1\rangle|0\rangle]$$

Algoritmo di Grover

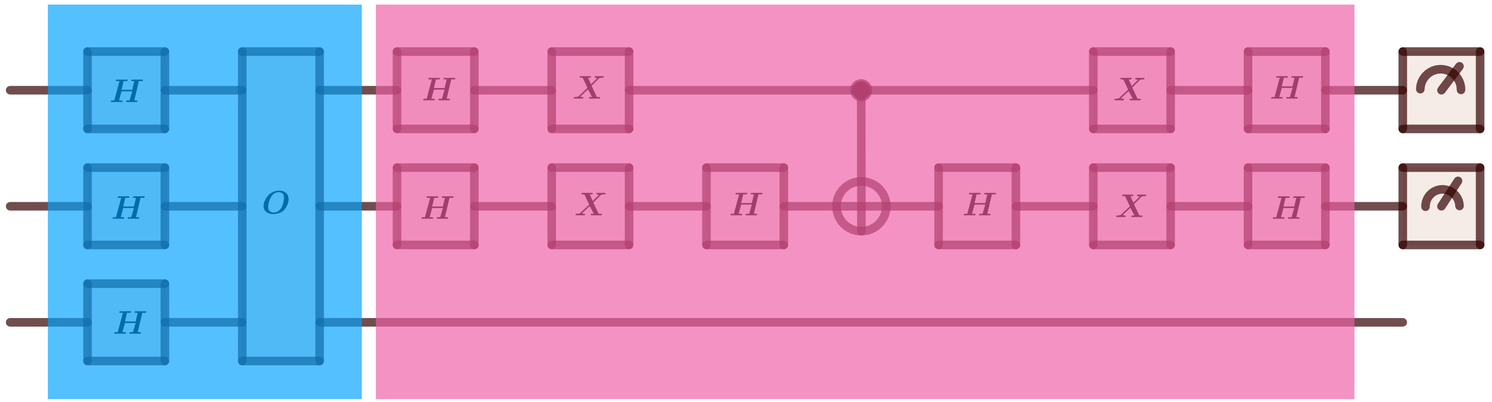


$$\frac{1}{\sqrt{2}}[|0\rangle|0\rangle - |1\rangle|0\rangle] \xrightarrow{I \otimes H} \frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |1\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right]$$

$$\frac{1}{\sqrt{2}}\left[|0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |1\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right] \xrightarrow{X \otimes X} \frac{1}{\sqrt{2}}\left[|1\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right]$$

$$\frac{1}{\sqrt{2}}\left[|1\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) - |0\rangle\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\right] \xrightarrow{H \otimes H} -|1\rangle|0\rangle \xrightarrow{Misura} P(1,0) = 1$$

Algoritmo di Grover



$$|\psi_1\rangle = \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle - |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right] \xrightarrow{Misura} P(0,0) = P(1,0) = P(0,1) = P(1,1)$$

$$|\psi_{fin}\rangle = -|1\rangle|0\rangle \xrightarrow{Misura} P(1,0) = 1$$

Abbiamo implementato f UNA SOLA VOLTA!!!

Possiamo rileggere quanto visto
da un punto di vista geometrico

Algoritmo di Grover

Interpretazione geometrica

Abbiamo visto lo stato che codifica i quattro elementi

$$|\psi_0\rangle = \left[\frac{1}{2}\left(|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|0\rangle + |1\rangle|1\rangle\right)\right]$$

Possiamo riscrivere questo stato in modo che sia somma di due vettori unitari di cui uno è proprio lo stato che codifica l'elemento cercato

$$= \frac{\sqrt{3}}{2}\left(\frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{3}}\right) + \frac{1}{2}(|1\rangle|0\rangle)$$

$$|u\rangle = \frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{3}} \qquad |x_0\rangle = |1\rangle|0\rangle$$

Algoritmo di Grover

Interpretazione geometrica

$$|\psi_0\rangle = \frac{\sqrt{3}}{2}\left(\frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{3}}\right) + \frac{1}{2}(|1\rangle|0\rangle)$$

$$|\psi_0\rangle = \frac{\sqrt{3}}{2}|u\rangle + \frac{1}{2}|x_0\rangle$$

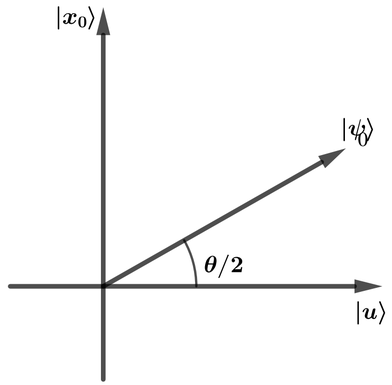
$$|\psi_0\rangle = cos\frac{\theta}{2}|u\rangle + sin\frac{\theta}{2}|x_0\rangle \longrightarrow |\psi_0\rangle = (cos\frac{\theta}{2}, sin\frac{\theta}{2})$$

$$\frac{\theta}{2} = 30°$$

Nel piano generato dai vettori ortogonali $|u\rangle$ e $|x_0\rangle$

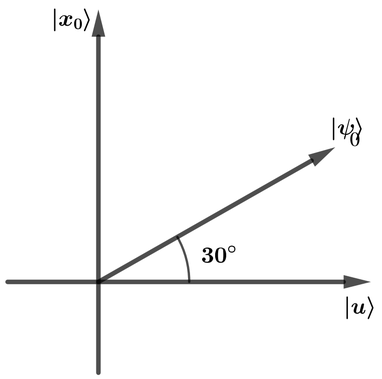
Algoritmo di Grover

Interpretazione geometrica



$$|\psi_0\rangle = cos\frac{\theta}{2}|u\rangle + sin\frac{\theta}{2}|x_0\rangle$$

$$|\psi_0\rangle = \left(cos\frac{\theta}{2}, sin\frac{\theta}{2}\right)$$

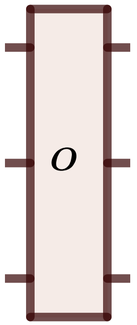


$$|\psi_0\rangle = \frac{\sqrt{3}}{2}|u\rangle + \frac{1}{2}|x_0\rangle$$

$$|\psi_0\rangle = \left(\frac{\sqrt{3}}{2}, \frac{1}{2}\right)$$

Algoritmo di Grover

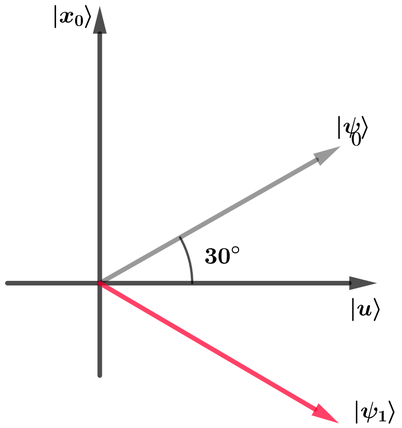
Interpretazione geometrica



$$|\psi_1\rangle = \frac{\sqrt{3}}{2}\left(\frac{|0\rangle|0\rangle + |0\rangle|1\rangle + |1\rangle|1\rangle}{\sqrt{3}}\right) - \frac{1}{2}(|1\rangle|0\rangle)$$

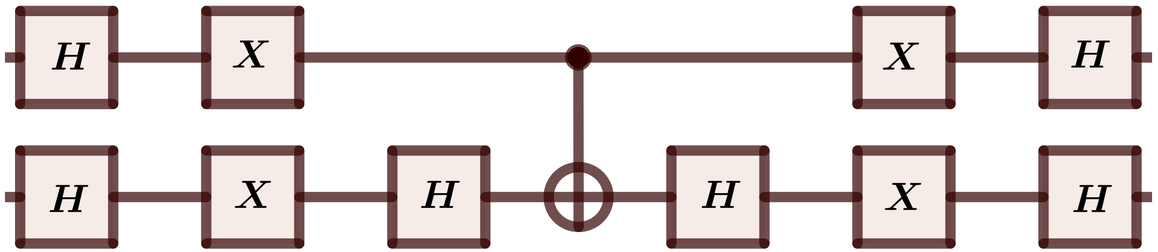
$$|\psi_1\rangle = \left(\frac{\sqrt{3}}{2}, -\frac{1}{2}\right)$$

Riflessione rispetto $|u\rangle$

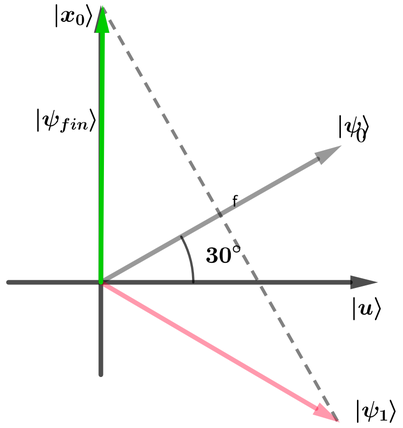


Algoritmo di Grover

Interpretazione geometrica



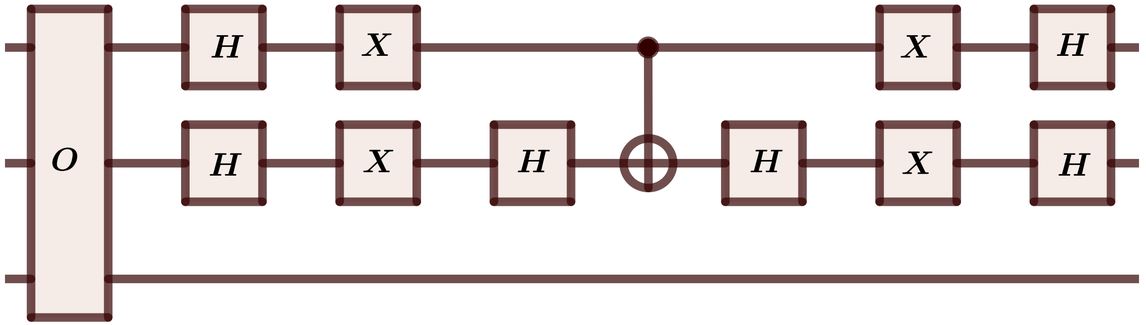
Riflessione rispetto $|\psi_0\rangle$



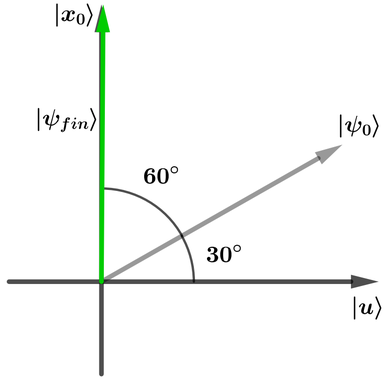
$$|\psi_{fin}\rangle = |x_0\rangle$$

Algoritmo di Grover

Interpretazione geometrica



Operatore di Grover **G**



2 Riflessioni = 1 Rotazione $\quad \frac{\theta}{2} \cdot 2$

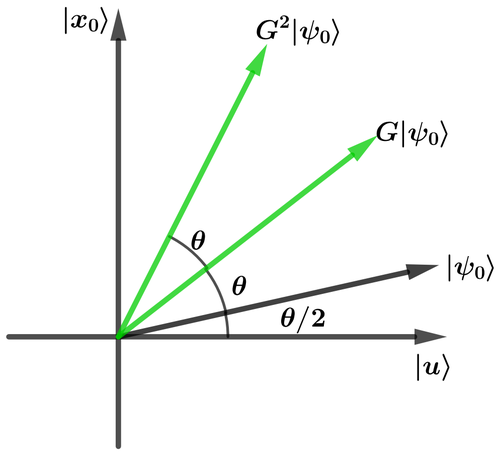
$$G|\psi_0\rangle = cos\left((3)\frac{\theta}{2}\right)|u\rangle + sin\left((3)\frac{\theta}{2}\right)|x_0\rangle$$

$$P(x_0) = sin^2 90° = 1$$

Algoritmo di Grover

Interpretazione geometrica

Operatore di Grover **G**



M **M**

Se cerchiamo M elementi!!!

$$|\psi_0\rangle = \sqrt{\frac{2^n - 1}{2^n}}\,|u\rangle + \sqrt{\frac{1}{2^n}}\,|x_0\rangle$$

$$G^k|\psi_0\rangle = cos\left((2k+1)\frac{\theta}{2}\right)|u\rangle + sin\left((2k+1)\frac{\theta}{2}\right)|x_0\rangle$$

$$sin^2\left((2k+1)\frac{\theta}{2}\right) = P(x_0)$$

$k = \sqrt{2^n}$ ⟶ **In media implementiamo** f $\sqrt{2^n}$ **volte**

Esercizio: Per $n = 3$ Determinare la probabilità di ottenere l'elemento cercato dopo aver applicato una volta l'operatore di Grover; fare la stessa cosa dopo aver applicato due volte l'operatore di Grover.

Algoritmo di Grover

$$\sqrt{2^n} = ?$$

Un’importantissima applicazione dell'algoritmo di Grover e' nel campo della crittoanalisi. Si richiede in alcuni casi particolari (attacco con approccio a forza bruta) una ricerca tra tutte le $2^{56} = 7 \times 10^{16}$ possibili chiavi.
Un computer classico, potendo esaminarne ad esempio 1 milione al secondo, impiegherebbe migliaia di anni (2000 anni c.a.) a scoprire quella corretta; un computer quantistico che utilizzi l'algoritmo di Grover, invece, ci metterebbe circa 4 minuti.

Algoritmo di Grover

Possibile percorso didattico

Algoritmi di ricerca:

1. Gli algoritmi di ricerca in generale
2. La ricerca in un array non ordinato: ricerca sequenziale
3. La ricerca in un array ordinato: ricerca sequenziale
4. La ricerca in un array ordinato: ricerca binaria

   Approfondimenti (Problema delle 8 regine)
   https://artificial-intelligence.unibs.it/didattica-IA/wp-content/uploads/IntroRicerca20154.pdf

5. Algoritmo di ricerca quantistico

Nei prossimi 3 mesi

1. Interviste
2. Tempo per rivedere quanto introdotto e svolgere gli esercizi (cartella)
3. Organizzare gruppi di lavoro coordinati con due scopi:
    A. Riflettere sugli argomenti trattati ipotizzando anche ulteriori sviluppi
    B. Lavorare sulla produzione di materiali adatti alle lezioni con gli studenti

Bibliografia essenziale

Nielsen, M. A., & Chuang, I. (2002). Quantum computation and quantum information.

Deutsch, D. (1985). Quantum theory, the Church–Turing principle and the universal quantum computer. *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, *400*(1818), 97-117.

Benenti, G., Casati, G., Rossini, D., & Strini, G. (2018). Principles of Quantum Computation and Information: A Comprehensive Textbook. World scientific.

Hill, R. K. (2016). What an algorithm is. *Philosophy & Technology*, *29*(1), 35-59.

Strubell, E. (2011). An introduction to quantum algorithms. *COS498 Chawathe Spring*, *13*, 19.

De Oliveira, A. N., Walborn, S. P., & Monken, C. H. (2005). Implementing the Deutsch algorithm with polarization and transverse spatial modes. *Journal of Optics B: Quantum and Semiclassical Optics*, *7*(9), 288.

Cleve, R., Ekert, A., Macchiavello, C., & Mosca, M. (1998). Quantum algorithms revisited. Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences, 454(1969), 339-354.

Perry, A., Sun, R., Hughes, C., Isaacson, J., & Turner, J. (2019). Quantum Computing as a High School Module. *arXiv preprint arXiv:1905.00282*.

T. Rudolph, Quanti, Ed. Adelphi

Grover, L. K. (1996). A fast quantum mechanical algorithm for estimating the median. *arXiv preprint quant-ph/9607024*.

Lavor, C., Manssur, L. R. U., & Portugal, R. (2003). Grover's Algorithm: quantum database search. *arXiv preprint quant-ph/0301079*.