Deutsch's - Josza : (1985 - 1992)

È un algoritmo deterministico uno dei primi esempi di algoritmi quantistici esponenzialmente più veloci di ogni possibile algoritmo deterministico.

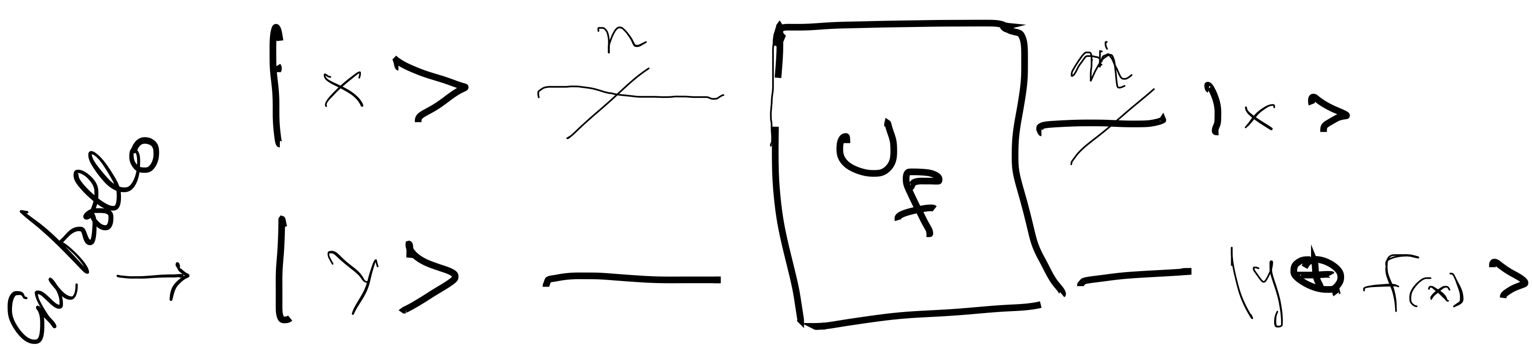
Dato: un ORACOLO che implementa una funzione booleana $f:\{0,1\}^n \to \{0,1\}$ che è costante o bilanciata ($\#0 = \#1$)

GOAL Decidere se f costante o bilanciata

<u>Oss</u> Un algoritmo <u>deterministico</u> classico richiede $\underline{2^{n-1}+1}$ interrogazioni (se n # bits).

Vediamo che con l'algoritmo quantistico D-J basta 1 solo interrogazione.

Se l'oracolo è il seguente



basta usare $\underline{\boxed{U_f}}$ solo 1 volta!

Vediamo più in dettaglio:

- Sia $|0\rangle^{\otimes n}|1\rangle$ lo stato di $n+1$ qbits.

- Applichiamo Hadamard e otteniamo

$$(*)\quad |0\rangle^{\otimes n}|1\rangle \xrightarrow{H^{\otimes n+1}} \frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{2^n-1}|i\rangle(|0\rangle-|1\rangle)$$

- Applichiamo l'oracolo che implementa f

$$|x\rangle|y\rangle \xrightarrow{O} |x\rangle|y\oplus f(x)\rangle \quad a \ (*)$$

otteniamo

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{2^n-1}|i\rangle(|f(i)\rangle-|1\oplus f(i)\rangle) =$$

$$\frac{1}{\sqrt{2^{n+1}}}\sum_{i=0}^{2^n-1}(-1)^{(i)}|i\rangle(|0\rangle-|1\rangle)$$

- Possiamo ignorare l'ultimo q-bit

- $$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \cdot |i>$$

- applicando H a ogni Q bit

$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} (-1)^{f(i)} \left[\frac{1}{\sqrt{2^n}} \sum_{j=0}^{2^n-1} (-1)^{ij} \, |j> \right] =$$

$$\frac{1}{2^n} \sum_{j=0}^{2^n-1} \left(\sum_{i=0}^{2^n-1} (-1)^{f(i)} (-1)^{ij} \right) |j> .$$

Da cui segue che la probabilità di misurare $|0\rangle^{\otimes n}$ è

$$\left|\frac{1}{2^n}\sum_{i=0}^{2^n-1}(-1)^{f(i)}\right|^2$$

che è uguale a 1 se f è costante e 0 se f è bilanciata.

—

Esempio

Supponiamo di avere le funzioni

$$f_1(x,y) = (x,y) \qquad f_3(x,y) = (x, x \oplus y)$$

$$f_2(x,y) = (x, \neg y) \qquad f_4(x,y) = (x, x \oplus (\neg y))$$

$x, y \in \{0,1\}$. Vogliamo distinguere le prime due funzioni dalle altre:

Se $S_1 = \{f_1, f_2\}$, $S_2 = \{f_3, f_3\}$ e una black box implementa f una delle f_i vogliamo decidere se f è in S_1 o S_2.

Dal momento che:

$$f_1(0,0) = f_3(0,0) = (0,0)$$
$$f_2(0,0) = f_4(0,0) = (0,1)$$

non basta Val $(0,0)$

ma nemmeno in $(1,1)$, $(1,0)$ o $(0,1)$!

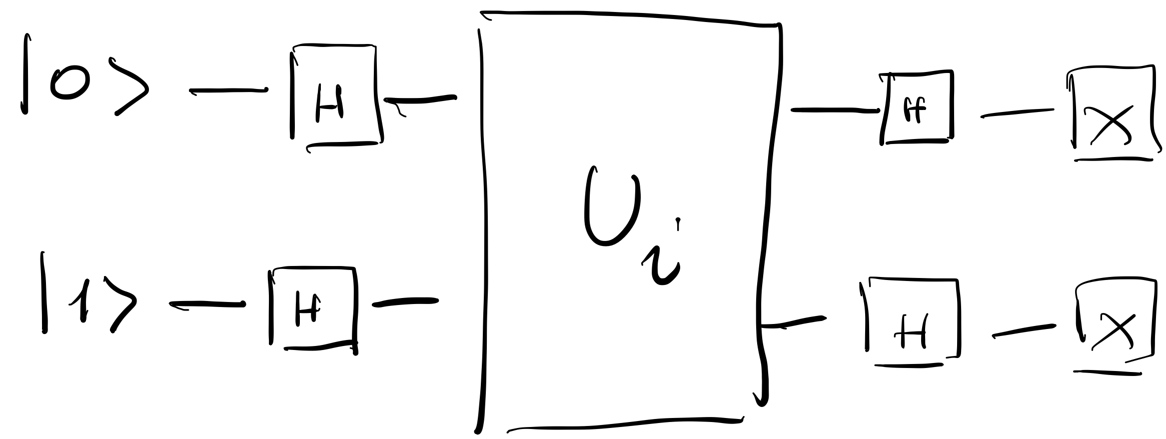
ci vogliono almeno 2 valutazioni.

Se operiamo in "quantum mode"?

1. Passo: implementiamo le f_i come gate quantistici

$$U_1 = I \quad U_2 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \quad U_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$U_4 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ e definiamo



Che succede ?

$$|0\rangle|1\rangle \longrightarrow \psi = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\left(\frac{1}{\sqrt{2}}|0\rangle-|1\rangle\right) =$$

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

Se applichiamo U_i

$$|\psi_1\rangle = U_1|\psi\rangle = \psi$$

$$|\psi_2\rangle = U_2|\psi\rangle = \frac{1}{2}(-|00\rangle+|01\rangle-|10\rangle+|11\rangle)$$

$$|\psi_3\rangle = U_3|\psi\rangle = \frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)$$

$$|\psi_4\rangle = U_4|\psi\rangle = \frac{1}{2}(-|00\rangle+|01\rangle+|10\rangle-|11\rangle)$$

Se poi riapplichiamo

$$H^{\otimes 2} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Si ha:

$$|\chi_1\rangle = H^{\otimes 2} U_1 |\psi\rangle = |01\rangle$$

$$|\chi_2\rangle = H^{\otimes 2} |\psi_2\rangle = -|01\rangle$$

$$|\chi_3\rangle = H^{\otimes 2} |\psi_3\rangle = |11\rangle$$

$$|\chi_4\rangle = H^{\otimes 2} |\psi_4\rangle = -|11\rangle$$

Se quindi misuriamo otteniamo

$|01\rangle$ se $f \in S_1$

$|11\rangle$ se $f \in S_2$!

Deutsch Algorithm

È un caso speciale per $n = 1$

Se $f : \{0,1\} \to \{0,1\}$ per

decidere se f è costante

basta vedere se $f(0) = f(1)$

$\iff$ vedere il valore $f(0) \oplus f(1)$

Se $= 0$ allora f costante.

aggiungiamo un qbit e

partiamo con $|0\rangle|1\rangle$

Applichiamo a ogni qbit H e otteniamo

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

Come visto prima usiamo l'implementazione quantistica di f

$$|x\rangle|y\rangle \longrightarrow |x\rangle|f(x)\oplus y\rangle$$

Se applichiamo a $*$ otteniamo

$$\frac{1}{2}\Big(|0\rangle\big(|f(0)\oplus 0\rangle - |f(0)\oplus 1\rangle\big) +$$

$$|1\rangle\big(|f(1)\oplus 0\rangle - |f(1)\oplus 1\rangle\big)\Big) =$$

$$= \frac{1}{2}\Big((-1)^{f(0)}|0\rangle\big(|0\rangle - |1\rangle\big) +$$

$$(-1)^{f(1)}|1\rangle\big(|0\rangle - |1\rangle\big)\Big) =$$

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

Se ignoriamo l'ultimo bit e la fase

$$\frac{1}{\sqrt{2}}\Big(|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle\Big)$$

Applicando H:

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

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

Da cui $f(0)\oplus f(1) = 0 \Leftrightarrow$ misuriamo uno 0 e $f(0)\oplus f(1) = 1 \Leftrightarrow$ misuriamo un 1.