Algoritmo di Grover.

∴ Trovare un elemento in un insieme non strutturato di N el.

Algoritmo classico $O(N)$

Grover: $O(\sqrt{N})$ =

È stato provato che è <u>ottimale</u>

Impostazione:

1. $\#A = N = 2^n$

2. Assegnamo a ogni elemento di A un indice $x \in \{0, 2^n - 1\}$.

3. Supponiamo esistano esattamente M soluzioni, $1 \leq M \leq N$

4. Supponiamo esista un <u>ORACOLO</u> che riconosce se una data sequenza di n-bits sia soluzione o no. Ossia esiste una trasformazione unitaria O che implementa

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

t.c. $f(x) = 1$ se x è soluzione
$f(x) = 0$ se non è soluzione

L'oracolo è realizzato dalla trasformazione unitaria

$$O : |x\rangle|q\rangle \longrightarrow |x\rangle|q \oplus f(x)\rangle$$

$x \in \{0,1\}^n$ ↑ singolo qbit

Se $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = H|1\rangle$

$$O(|x\rangle|q\rangle) = |x\rangle|\tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \oplus f(x)\rangle =$$

$$= |x\rangle\left(\tfrac{1}{\sqrt{2}}(|0\rangle \oplus f(x)\rangle - |1 \oplus f(x)\rangle\right) =$$

$$= \begin{cases} |x\rangle(\tfrac{1}{\sqrt{2}}|0\rangle - |1\rangle) = |x\rangle|q\rangle & f(x)=0 \\ |x\rangle(\tfrac{1}{\sqrt{2}}(|1\rangle - |0\rangle) = -|x\rangle|q\rangle & f(x)=1 \end{cases}$$

inverte le ampiezze degli stati che sono soluzioni!

Possiamo riscrivere come:

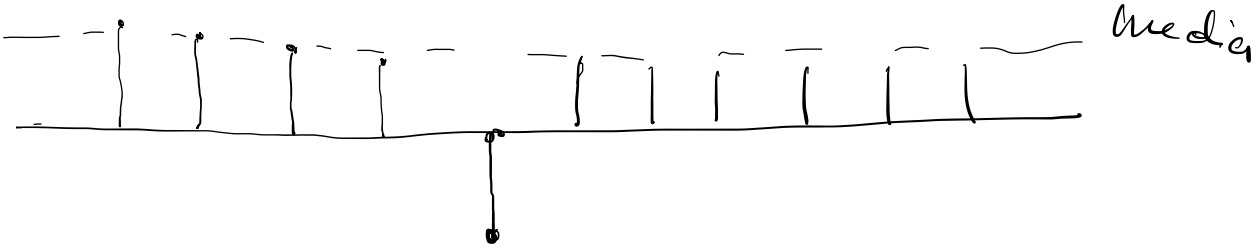
$$O(|x\rangle|1/\sqrt{2}(|0\rangle-|1\rangle)=(-1)^{f(x)}|x\rangle|1/\sqrt{2}(|0\rangle-|1\rangle)$$

↑ uscirà modificato

quindi nella descrizione faremo ignorando e scriveremo

$$O\left(\sum_{x=0}^{2^n-1}\alpha_x|x\rangle\right)=\sum_{x=0}^{2^{n-1}}(-1)^{f(x)}\alpha_x|x\rangle$$

Es $M=1$ effetto di O sulla superposizione



Algoritmo di Grover

Consideriamo l'operatore P_0 t.c. per $0 \le x \le N-1$

$$P_0 |x\rangle \longrightarrow \begin{cases} |x\rangle & \text{se } x = 0 \\ -|x\rangle & \text{se } x \neq 0 \end{cases}$$

ossia P_0 esegue uno shift di fase -1 su tutti gli stati computazionali $\neq |0\rangle$

Oss. Se consideriamo l'operatore inverso

$$(2|0\rangle\langle 0| - I)(\alpha|0\rangle + \beta|1\rangle) =$$

$$2\alpha \underbrace{\langle 0|0\rangle}_{1}|0\rangle + 2\beta \underbrace{\langle 0|1\rangle}_{0}|1\rangle - \alpha|0\rangle - \beta|1\rangle =$$

$$\alpha|0\rangle - \beta|1\rangle = \underline{\underline{P_0}}\,(\alpha|0\rangle + \beta|1\rangle)$$

Se quindi $|s\rangle = H^{\otimes n}|0\rangle =$

$$= \frac{1}{\sqrt{N}} \sum_{0}^{N-1} |x\rangle$$

si ha che

$$H^{\otimes n} P_0 H^{\otimes n} = H^{\otimes n}(2|0\rangle\langle 0| - I) H^{\otimes n}$$

$$= 2|s\rangle\langle s| - I$$

operatore di diffusione di Grover

Definiamo OPERATORE di GROVER

$$G = H^{\otimes n} P_0 H^{\otimes n} \cdot O =$$

$$= (2|s\rangle\langle s| - I) O$$

Algoritmo di Grover

1. Inizializzare il sistema nello stato

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

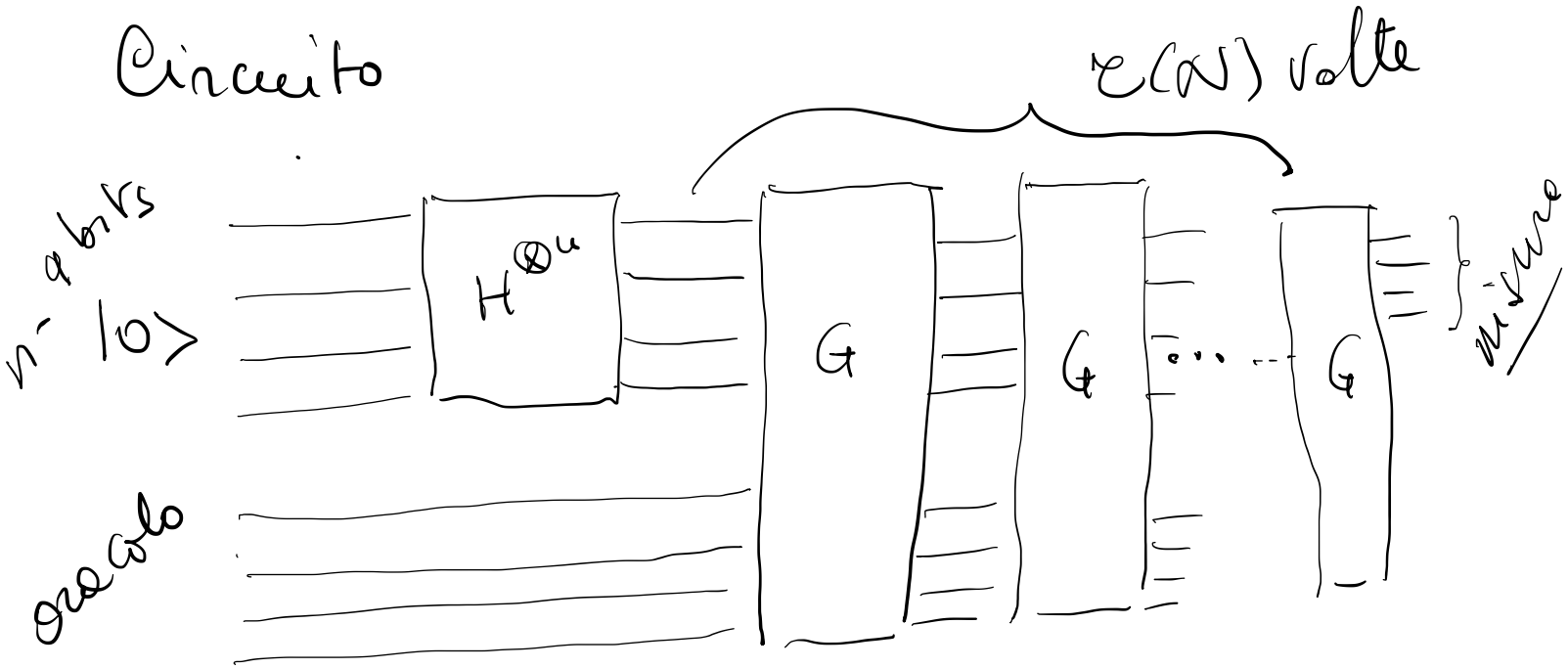
2. Ripetere $r(N)$ volte:

"ITERAZIONE DI GROVER"

a. Applica O
b. Applica $2|s\rangle\langle s| - I$ } G

3. misurare il risultato.

Circuito



OSSERVAZIONE

Se applichiamo a uno stato

$$\sum_{x=0}^{N-1} \alpha_x |x\rangle$$ l'operatore $2|s\rangle\langle s| - I$

otteniamo:

$$\left(2|s\rangle\langle s| - I\right) \sum_{0}^{N-1} \alpha_x |x\rangle =$$

$$2 \sum_{0}^{N-1} \alpha_x \langle s|x\rangle |s\rangle - \sum \alpha_x |x\rangle =$$

$\langle s|x\rangle = 1/\sqrt{N}$

$$2 \sum_{x}^{N-1} \frac{\alpha_x}{\sqrt{N}} \cdot \left(\frac{1}{\sqrt{N}} \sum |x\rangle\right) - \sum \alpha_x |x\rangle =$$

$$\sum_x \left(2 \left(\frac{\sum \alpha_x}{N} \right) - \alpha_x \right) |x\rangle$$

$\frac{\sum \alpha_x}{N}$ → media degli α_x

inversione rispetto alla media!

Cominciamo con il caso $N=1$

Sia β l'elemento che cerchiamo.

Allora O è rappresentato da un Operatore U_β (dimostrando ugualmente)

$$U_\beta |x\rangle = (-1)^{f(x)} \cdot |x\rangle = \begin{cases} |x\rangle & x \neq \beta \\ -|x\rangle & x = \beta \end{cases}$$

ma si ha anche

$$(I - 2|\beta\rangle\langle\beta|)|x\rangle = |x\rangle - 2\langle\beta|x\rangle|\beta\rangle$$

$$= \begin{cases} |x\rangle & x \neq \beta \\ -|x\rangle & x = \beta \end{cases}$$

$$G = (2|s\rangle\langle s| - I)(I - 2|\beta\rangle\langle\beta|)$$

Ma allora entrambe le trasformazioni sono Hadamard

Vediamo cosa succede al primo passo:

intanto $\langle \beta | s \rangle = \frac{1}{\sqrt{N}}$, $\langle s | s \rangle = N \cdot \frac{1}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} = 1$

Applichiamo U_β e poi $U_s = 2|s\rangle\langle s| - I$

$$U_\beta |s\rangle = (I - 2|\beta\rangle\langle\beta|)|s\rangle =$$

$$= |s\rangle - 2\langle\beta|s\rangle \cdot |\beta\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\beta\rangle$$

$$U_s\left(|s\rangle - \frac{2}{\sqrt{N}}|\beta\rangle\right) = \left(2|s\rangle\langle s| - I\right)\left(|s\rangle - \frac{2}{\sqrt{N}}|\beta\rangle\right) =$$

$$= 2\underbrace{\langle s|s\rangle}_{1}|s\rangle - \frac{4}{\sqrt{N}}\underbrace{\langle s|\beta\rangle}_{1/\sqrt{N}}|s\rangle - |s\rangle + \frac{2}{\sqrt{N}}|\beta\rangle =$$

$$= \frac{N-4}{N}|s\rangle + \frac{2}{\sqrt{N}}|\beta\rangle .$$

Se $N=4$ e misuriamo $U_s U_\beta |s\rangle = |\beta\rangle$

In generale se guardiamo l'ampiezza di $|\beta\rangle$ in $U_s U_\beta |s\rangle$ dopo il primo passo vediamo che $|\langle\beta|s\rangle|^2 = \frac{1}{N}$ è passata a

$$|\langle\beta, U_s U_\omega \beta\rangle|^2 = \left|\frac{1}{\sqrt{N}} \cdot \frac{N-4}{N} + \frac{2}{\sqrt{N}}\right|^2 =$$

$$= \frac{(3N-4)^2}{N^3} = 9\left(1-\frac{4}{3N}\right)^2 \cdot \frac{1}{N}$$

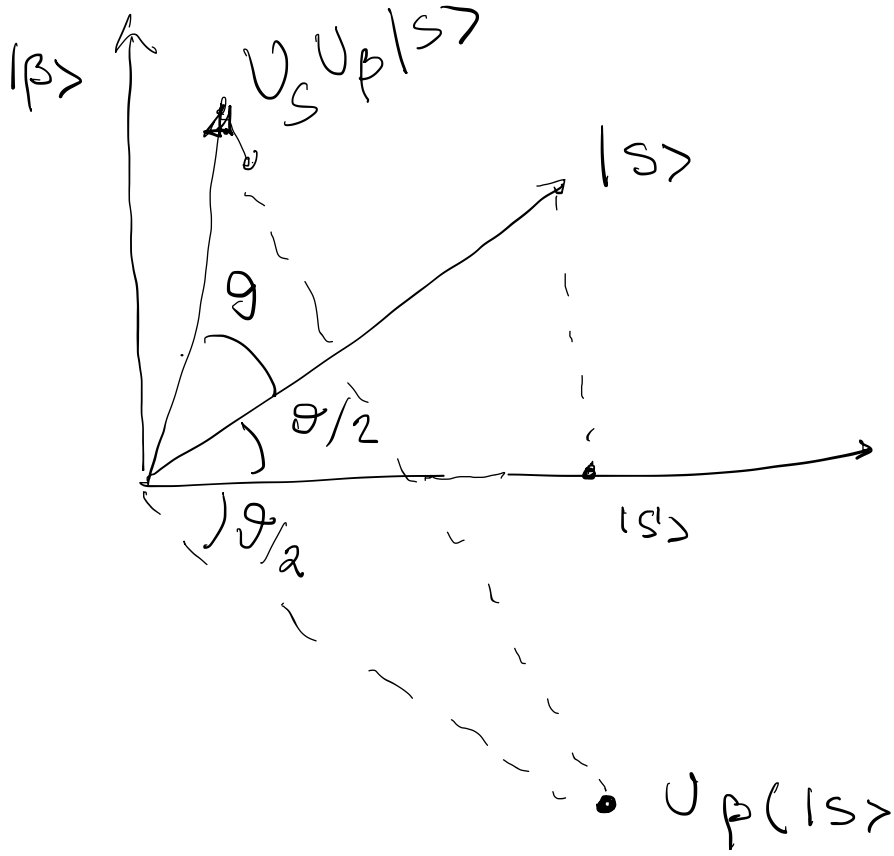
> 1 per $N > 2$

Quanti passi?

Interpretazione geometrica

Abbiamo osservato che sia U_β che U_S sono matrici di Householder e quindi rappresentano delle riflessioni rispetto all'"iperpiano" $|s\rangle$ e a quello $\perp$ a β rispettivamente

chiamiamo $|s'\rangle$ il ket ortogonale a β $\quad |s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \beta} |x\rangle$



Quindi se $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ e

$$|s'\rangle = \frac{1}{\sqrt{N-1}} \sum_{x \neq \beta} |x\rangle$$

si ha $\langle s | s' \rangle = \sqrt{\frac{N-1}{N}}$ e

$$\frac{\vartheta}{2} = \arccos \sqrt{\frac{N-1}{2}} = \arcsin \frac{1}{\sqrt{N}}$$

le riscrivere $|s\rangle = \cos\frac{\vartheta}{2} |s'\rangle + \sin\frac{\vartheta}{2} |\beta\rangle$

Con queste notazioni si ha allora che

$$G|s\rangle = \cos\left(\frac{3}{2}\vartheta\right)|s'\rangle + \sin\left(\frac{3}{2}\vartheta\right)|\beta\rangle$$ (*)

e de nella base $|s'\rangle |\beta\rangle$ vale

$$G = \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}$$

Iterando si ottiene

$$G^k(|s\rangle) = \cos\left(\frac{2k+1}{2}\vartheta\right)|s'\rangle + \sin\left(\frac{2k+1}{2}\vartheta\right)|\beta\rangle$$

quindi iterando si ottiene un devi vettore di stato $|s\rangle$ si "avvicina" a $|\beta\rangle$. Quando questo succede la probabilità di ottenere $|\beta\rangle$ dalla misurazione aumenta!

Quante iterazioni?

Vediamo di determinare il numero ottimale di volte.

$$0 = \cos\left(\frac{2k+1}{2}\vartheta\right) = \cos k\vartheta \cos\frac{\vartheta}{2} - \sin k\vartheta \sin\frac{\vartheta}{2} =$$

$$= \sqrt{\frac{N-1}{N}} \cos k\vartheta - \sqrt{\frac{1}{N}} \sin k\vartheta$$

da cui $\operatorname{tg} k\vartheta = \sqrt{N-1}$ e

(usando $1+\operatorname{tg}^2\alpha = \frac{1}{\cos^2 x}$) $\cos k\vartheta = \sqrt{\frac{1}{N}}$

$$\Rightarrow k_0 = \left\lfloor \frac{\arccos\sqrt{\frac{1}{N}}}{\vartheta} \right\rfloor = \left\lfloor \frac{\arccos\sqrt{\frac{1}{N}}}{2\arccos\sqrt{\frac{N-1}{N}}} \right\rfloor$$

$$\Rightarrow k_0 \simeq \frac{\sqrt{N}}{2} \arccos\sqrt{\frac{1}{N}} \simeq \frac{\pi}{4}\sqrt{N}$$

intero più vicino

Approssimando

$$\cos\frac{\vartheta}{2} = \sqrt{\frac{N-1}{N}} \simeq 1 - \frac{1}{2N} \simeq 1 - \frac{\vartheta^2}{8}$$

Quindi concludendo per ottenere la più alta probabilità bisogna iterare G un numero di volte $\Theta(\sqrt{N})$ infatti

$$\text{Prob}_{G^{k_0}|s\rangle}\{x=\beta\} = |\langle \beta | G^{k_0} | s \rangle\rangle|^2 =$$

$$\sin^2\left(\frac{2k_0+1}{2}\vartheta\right) \simeq \sin\left(\frac{\pi}{2} + \sqrt{\frac{1}{N}}\right)$$

$$\simeq 1 - \Theta\left(\frac{1}{N}\right)$$

ossia probabilità di errore $\Theta\left(\frac{1}{N}\right)$

Caso $M > 1$ - Sia S l'insieme degli x che sono soluzione
si possono ripetere i passi che abbiamo fatto considerando i vettori:

$$|S'\rangle = \sqrt{\frac{1}{N-M}} \sum_{x \notin S} |x\rangle$$

$$|t\rangle = \sqrt{\frac{1}{M}} \sum_{x \in S} |x\rangle$$

in questo modo

$$|S\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle = \sqrt{\frac{N-M}{N}} |S'\rangle + \sqrt{\frac{1}{M}} |t\rangle$$

di nuovo posto $\cos\frac{\vartheta}{2} = \langle S, S'\rangle = \sqrt{\frac{N-M}{N}}$

$$G|S\rangle = \cos\frac{\vartheta}{2}|S'\rangle + \sin\vartheta/2\,|t\rangle \quad e$$

$$G^k|S\rangle = \cos\left(\frac{2k+1}{2}\vartheta\right)|S'\rangle + \sin\left(\frac{2k+1}{2}\vartheta\right)|t\rangle$$

Con le dovute sostituzioni otteniamo

$$0 = \cos\left(\frac{2k_0+1}{2}\vartheta\right) = \sqrt{\frac{N-M}{N}}\cos\frac{k}{\vartheta} - \sqrt{\frac{M}{N}}\sin k\vartheta$$

da cui

$$k_0 = \left\lfloor \frac{\arccos\sqrt{\frac{M}{N}}}{\vartheta} \right\rfloor =$$

$$\left\lfloor \frac{\arccos\sqrt{\frac{M}{N}}}{2\arccos\sqrt{\frac{N-M}{N}}} \right\rfloor$$

$$\Rightarrow \quad k_0 \simeq \frac{\pi}{4}\sqrt{\frac{N}{M}} \qquad \text{se } N \gg M$$

Es $N = 8 = 2^3$ e cerchiamo

$\beta = 001$.

per descrivere questo sistema 3 qbits:

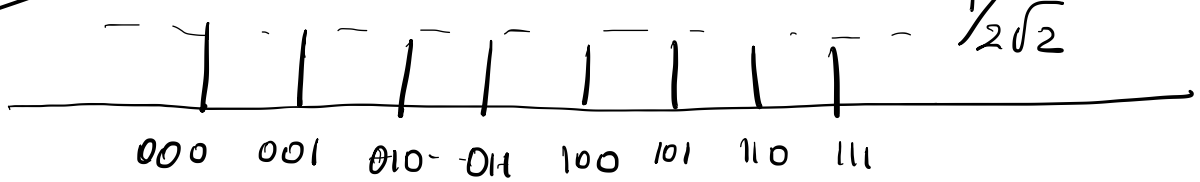
$$|\psi\rangle = \alpha_0 |000\rangle + \alpha_1 |001\rangle + \cdots + \alpha_7 |111\rangle$$

1. Passo

$$H^{\otimes 3} |000\rangle = \frac{1}{2\sqrt{2}} |000\rangle + \frac{1}{2\sqrt{2}} |001\rangle + \cdots + \frac{1}{\sqrt{2}} |111\rangle =$$

$$= \frac{1}{2\sqrt{2}} \sum_{x=0}^{7} |x\rangle = |s\rangle$$

Ampiezze



k_0 ottimale $\frac{\pi}{4}\sqrt{8} = \frac{2\pi}{4}\sqrt{2} \simeq 2.22$

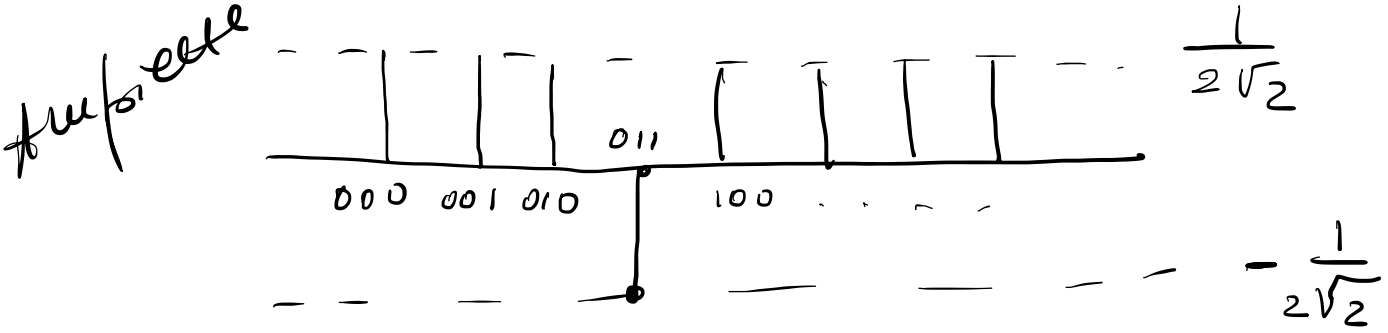
$\Rightarrow$ 2 iterazioni!

1 iterazione: oracolo, che vega l'accoppiata di $|011\rangle = \beta$

$$U_\beta |s\rangle = \frac{1}{2\sqrt{2}}|000\rangle + \frac{1}{2\sqrt{2}}|001\rangle + \dots \left(-\frac{1}{2\sqrt{2}}|011\rangle\right) + \frac{1}{2\sqrt{2}}|111\rangle$$

$$\text{con} \quad = |s\rangle - \frac{2}{2\sqrt{2}}\cdot|011\rangle$$

ampiezze

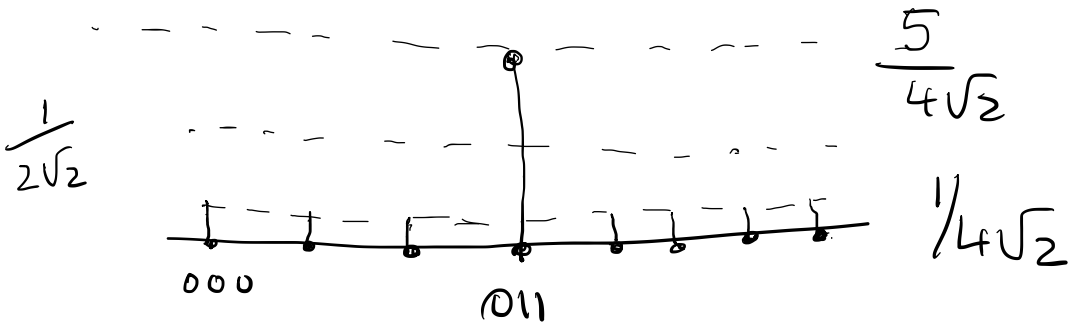


operatore di diffusione

$$(2|s\rangle\langle s| - I)\left(|s\rangle - \frac{1}{\sqrt{2}}|\beta\rangle\right) = \frac{1}{2}|s\rangle + \frac{1}{\sqrt{2}}|\beta\rangle =$$

$$= \frac{1}{2}\left[\frac{1}{2\sqrt{2}}\sum_{0}^{7}|x\rangle\right] + \frac{1}{\sqrt{2}}|011\rangle =$$

$$= \frac{1}{4\sqrt{2}}\sum_{\substack{0 \\ x\neq 3}}^{7}|x\rangle + \frac{5}{4\sqrt{2}}|011\rangle = |S_1\rangle$$



2ª iterazione

riapplicando U_β si ottiene

$$U_\beta|S_1\rangle = \frac{1}{4\sqrt{2}}\sum_{x\neq 3}|x\rangle - \frac{5}{4\sqrt{2}}|011\rangle =$$

$$= \frac{1}{4\sqrt{2}}\sum_{0}^{7}|x\rangle - \frac{6}{4\sqrt{2}}|011\rangle =$$

$$= \frac{1}{2}|S\rangle - \frac{3}{2\sqrt{2}}|011\rangle$$

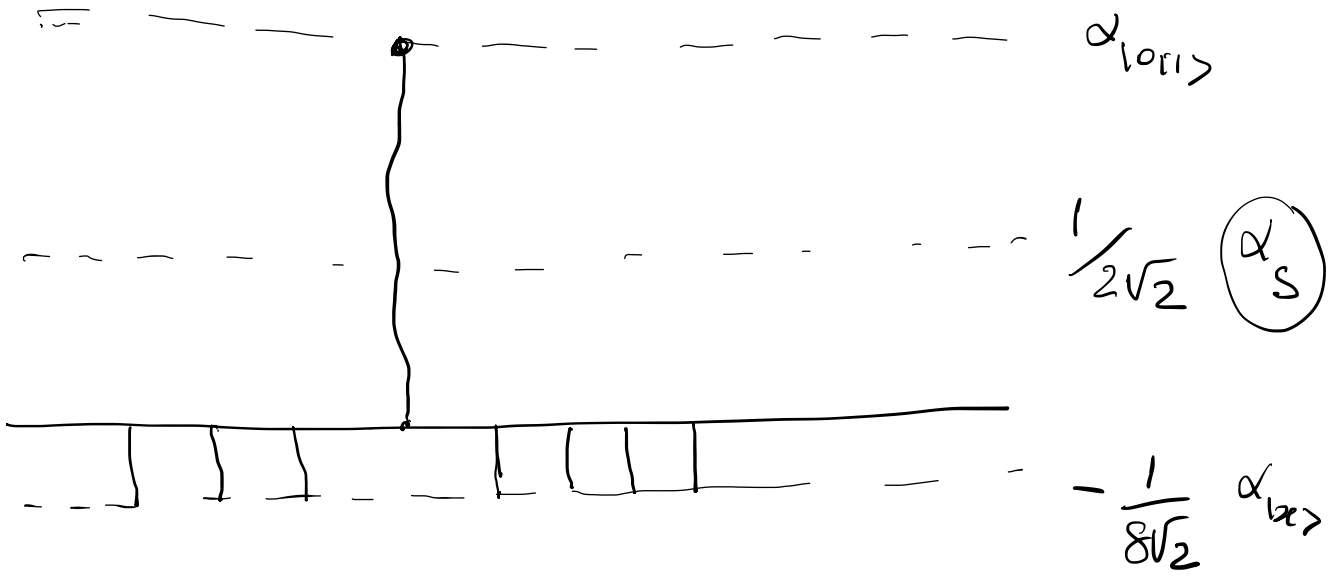
Dopo U_β applichiamo U_s

$$(2|s\rangle\langle s| - I)\left(\frac{1}{2}|s\rangle - \frac{3}{2\sqrt{2}}|011\rangle\right) =$$

$$= -\frac{1}{4}|s\rangle + \frac{3}{2\sqrt{2}}|011\rangle =$$

$$= -\frac{1}{4}\left[\frac{1}{2\sqrt{2}}\sum_{x\neq 3}|x\rangle + \frac{1}{2\sqrt{2}}|011\rangle\right] + \frac{3}{2\sqrt{2}}|011\rangle =$$

$$= -\frac{1}{8\sqrt{2}}\sum_{x\neq 3}|x\rangle + \frac{11}{8\sqrt{2}}|011\rangle$$



Se ora osserviamo il sistema la probabilità che lo stato che rappresenta la soluzione $|01\rangle$ sia misurato è

$$\left| \frac{11}{8\sqrt{2}} \right|^2 = \frac{121}{128} \simeq 94.5\%$$

mentre quella di trovare uno stato sbagliato è

$$\left| \frac{-\sqrt{7}}{8\sqrt{2}} \right|^2 = \frac{7}{128} \simeq 5.5\%$$

Se N aumenta l'errore diventa molto piccolo.

Algoritmo di Simon.

Problema di Simon:

Data una funzione $f: \{0,1\}^n \to \{0,1\}^n$

t.c $f(x) = f(y) \iff y = x \oplus s$

per $s \in \{0,1\}^n$, trovare s.

L'algoritmo che calcola s dato f (U_f come black-box) è stato uno dei primi algoritmi quantistici che ha risolto il problema in tempo polinomiale, con $O(n)$ interrogazioni U_f, mentre i

vettori alla base richiedono

$O(q^{n/2})$ chiamate di U_f.

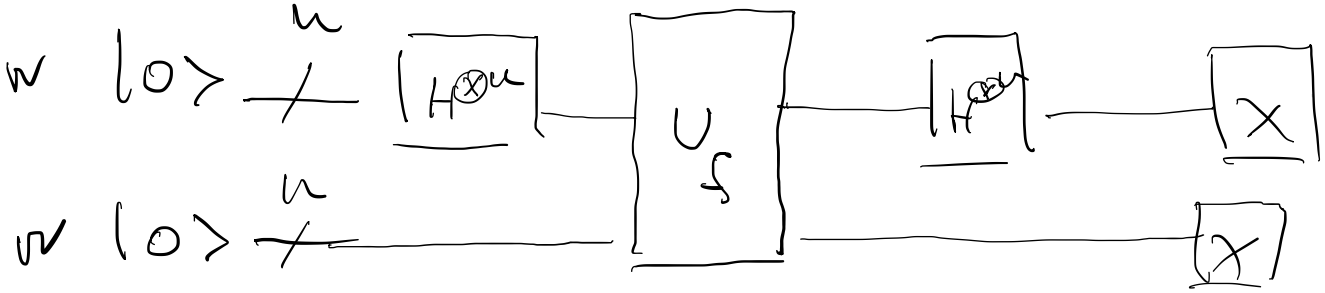
È anche un esempio di come usare gli algoritmi quantistici combinandoli con calcoli classici. Questo algoritmo si compone di 2 parti: una parte quantistica seguita poi da un algoritmo (classico) per la risoluzione di un sistema lineare.

La parte quantistica produce $n-1$ vettori linearmente ind.

$y_1 \dots y_{n-1}$ t.c. $y_i s = 0 \; \forall i$

Risolvendo il sistema (con metodi classici) si trova s.

Circuito:



1. Si parte usando $|0\rangle^{\otimes n} |0\rangle^{\otimes n}$ quindi 2 registri di n qubit

2. Si applica $H^{\otimes n}$ al primo registro

$$H^{\otimes n} |0\rangle |0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle |0\rangle$$

3. Poi si applica U_f

ad entrambi i registri e quindi

si ottiene

$$U_f\left(\frac{1}{\sqrt{N}}\sum_{0}^{N-1}|x\rangle|0\rangle\right) =$$

$$\frac{1}{\sqrt{N}}\sum_{0}^{N-1}|x\rangle|f(x)\rangle .$$

(l'oracolo è implementato come visto prima in modo che

$U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$ così

$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle$)

4. Si misura il 2 registro : ci sono 2 casi

a) $s = 0^n$

b) $s \neq 0^n$

se $s = 0^n \Rightarrow$ f è costante e quindi

Valne di x corrisponde ad una sola f(x)
e quindi il primo registro rimane
nella stessa sovrapposizione
e $\forall f(x)$ memorizzato x è una qualunque
elemento di $\{0,1\}^n$ con la stessa
ampiezza.

Se $S \neq 0^n$ misurando il secondo
registro si ottiene un valore $f(z)$
che limita i valori possibili per
il primo registro: ci sono solo
2 valori possibili per x: z e $z \oplus s$.
Quindi dopo la misurazione lo
stato del primo registro è

$$\frac{1}{\sqrt{2}}|z\rangle + \frac{1}{\sqrt{2}}|z \oplus s\rangle$$

Da ora in poi non si usa più il secondo registro e non lo considereremo.

Dobbiamo recuperare s.

Ricordiamo:

Es. $H^{\otimes n}|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{x \cdot y} |y\rangle$

dove $x \cdot y = x_1 y_1 \oplus \dots \oplus x_n y_n$.

Se applichiamo $H^{\otimes n}$ al primo registro:

$$H^{\otimes n}\left(\frac{1}{\sqrt{2}}|z\rangle + \frac{1}{\sqrt{2}}|z \oplus s\rangle\right) =$$

$$\frac{1}{\sqrt{2}} H^{\otimes n}|z\rangle + \frac{1}{\sqrt{2}} H^{\otimes n}|z \oplus s\rangle =$$

$$\frac{1}{\sqrt{2}} \left[\frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{z \cdot y} |y\rangle + \frac{1}{\sqrt{N}} \sum_{0}^{N-1} (-1)^{y \cdot (z+s)} |y\rangle\right]$$

$$= \frac{1}{\sqrt{2N}} \sum_{y=0}^{N-1} (-1)^{2y} \left[1 + (-1)^{s_y}\right] |y\rangle \quad *$$

ove ricordiamo il primo registro

- Se $s = 0^n \rightarrow$ stringa di distribuzione uniforme

- Se $s \neq 0^n$ (ossia $x \oplus y \neq 0^n$)

si può avere $s_y = 0$ o $s_y = 1$

- Se $s_y = 1$ * diviene

$$\frac{1}{\sqrt{2N}} \sum_{0}^{N-1} (-1)^{2y} \cdot 0 \cdot |y\rangle$$

quindi l'ampiezza è 0 e

un tale y non sarà mai misurato

vediamo solo stati y, con $y_s = 0$

* diventa

$$\frac{2}{\sqrt{2^N}} \cdot \sum_{0}^{N-1} (-1)^{2y} |y\rangle$$

Quindi la misurazione produce

sempre un y con $y = 0$

e l'ampiezza associata a

ogni valore è

$$\left| \frac{1}{\sqrt{2^{n-1}}} \right|^2 = \frac{1}{2^{n-1}}$$

se eseguiamo $n-1$ volte

troviamo $y_1, \dots, y_{n-1} \in \{0,1\}^n$

t.c. $y_i \cdot s = 0$ -

Risolvendo il sistema lineare

si trova s.

Serve però che $y_1, \dots, y_{n-1}$ siano

linearmente indipendenti

ma:

la probabilità di trovare y_1

è $\frac{1}{2^{n-1}}$. Nell'iterazione

successiva la probabilità

di osservare un y_2 distinto è

$1 - \frac{1}{2^{n-1}}$ - La probabilità

di osservare $n-1$ valori distinti di f e quindi un bound inferiore per la probabilità di ottenere $n-1$ vettori linearmente indipendenti è

$$\prod \left[1 - \frac{1}{2^n} \right] \simeq .2887881 > \frac{1}{4}$$

Quindi basta ripetere l'algoritmo di Simon al più $4n$ volte!

Servono $O(n)$ interrogazioni U_f per determinare s

Esempio: $n = 3 \quad S = 110$

x	$f(x)$
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

partiamo con $|000\rangle|000\rangle$

applichiamo $H^{\otimes 3}$ al primo registro

$$H^{\otimes 3}|000\rangle|000\rangle = \frac{1}{2\sqrt{2}} \sum_{x=0}^{7} |x\rangle|000\rangle$$

interroghiamo l'oracolo e otteniamo

$$\frac{1}{2\sqrt{2}} \sum_{0}^{7} |x\rangle |f(x)\rangle$$

misuriamo il secondo registro

Supponiamo di trovare

$010 = f(001) = f(111)$ $\Rightarrow$ il 1° reg. è

$\frac{1}{\sqrt{2}}(|001\rangle + |111\rangle)$. Calcoliamo

$$H^{\otimes 3}\left(\frac{1}{\sqrt{2}}(|001\rangle + |111\rangle)\right) =$$

$$\frac{1}{\sqrt{2}}\left[\frac{1}{2\sqrt{2}} \sum_{0}^{7} (-1)^{001\cdot y} \cdot |y\rangle + \frac{1}{2\sqrt{2}} \sum_{0}^{7} (-1)^{111\cdot y} \cdot |y\rangle\right] \otimes$$

Calcoliamo per $y = 0, \dots, 7$ $001 \cdot y$ e

$111 \cdot y$.

	y	001	111
0	000	0	0
1	001	1	1
2	010	0	1
3	011	1	0
4	100	0	1
5	101	1	0
6	110	0	0
7	111	1	1

Da cui $\otimes = \frac{1}{2}(|0\rangle - |1\rangle + |6\rangle - |7\rangle)$

Misurando supponiamo di trovare $|1\rangle = |001\rangle = y_1$

Ripetiamo per trovare un altro valore e supponiamo di misurare $|7\rangle = |111\rangle$

A questo punto risolviamo

$$\begin{cases} s \cdot y_1 = s_1 \cdot 0 + s_2 \cdot 0 + s_3 \cdot 1 = s_3 \cdot 1 = 0 \\ s \cdot y_2 = s_1 + s_2 + s_3 = 0 \end{cases}$$

tra quelle

$$\begin{cases} S_3 = 0 \\ S_1 = S_2 \end{cases} \longrightarrow \begin{matrix} 000 \\ 110 \end{matrix}$$

la sol. diversa da 0 è

<u>110</u> che è il vettore S.