132-quantum-grover-algorithm-03

Quantum Computing

L'Algoritmo di Grover

1

1

l'algoritmo

- l'algoritmo di Grover esegue $O(\sqrt{N})$ iterazioni
- ad ogni iterazione esegue i seguenti due step
  - phase inversion
  - inversion about min
- l'algoritmo mantiene nel tempo una superposition del tipo $\sum_x \alpha_x |x\rangle$
- in ciò che segue assumiamo che $f(x^*) = 1$ cioè che l'elemento cercato sia x^*

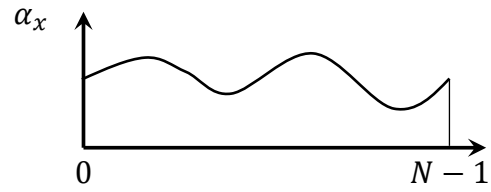
2

2

132-quantum-grover-algorithm-03

phase inversion

- rappresentiamo con un disegno i valori α_x ad un certo istante



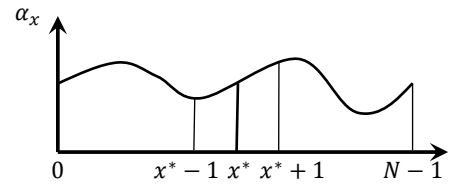
- se $x \neq x^*$ allora la phase inversion lascia il valore corrispondente di α_x invariato
- se $x = x^*$ allora la phase inversion trasforma α_{x^*} in $-\alpha_{x^*}$

3

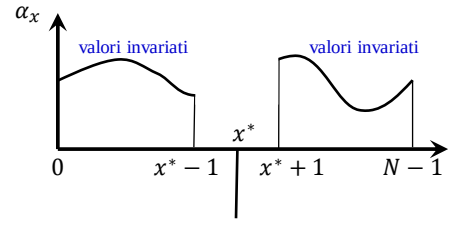
3

phase inversion

- prima della phase inversion



- dopo la phase inversion



4

4

132-quantum-grover-algorithm-03

inversion about mean

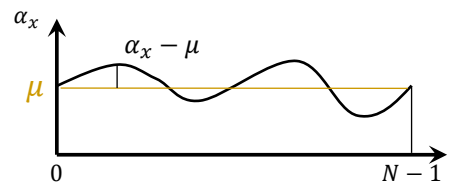
- consideriamo lo stato $\sum_x \alpha_x |x\rangle$ in un certo istante
- definiamo il *valor medio* μ come $\mu = \frac{\sum_{x=0}^{N-1} \alpha_x}{N}$
- inversion about mean fa il *flip* di ogni α_x attorno a μ, cioè trasforma ogni α_x in $2\mu - \alpha_x$
  - osserva che α_x può essere scritto come $\mu + (\alpha_x - \mu)$
- quindi lo stato $\sum_x \alpha_x |x\rangle$ è trasformato in $\sum_x (2\mu - \alpha_x) |x\rangle$

5

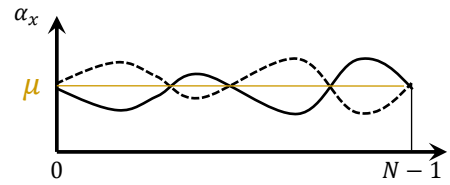
5

inversion about mean

- osserviamo che $2\mu - \alpha_x = \mu - (\alpha_x - \mu)$ quindi, dal punto di vista grafico
- prima dell'inversion about mean



- dopo l'inversion about mean



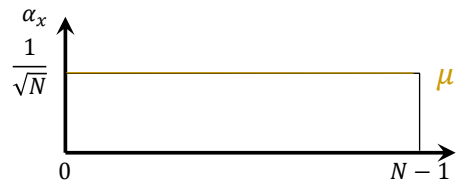
6

6

132-quantum-grover-algorithm-03

inizializzazione

- all'inizio imponiamo che tutte le ampiezze siano uguali a $\frac{1}{\sqrt{N}}$ e che quindi si parta dallo stato $\frac{1}{\sqrt{N}}\sum_x |x\rangle$
- dal punto di vista grafico abbiamo



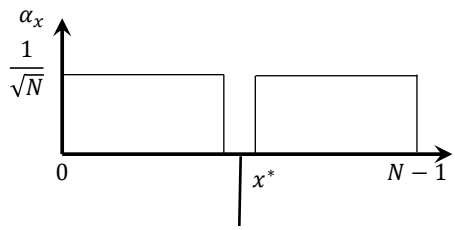
- abbiamo inoltre che $\mu = \frac{1}{\sqrt{N}}$

7

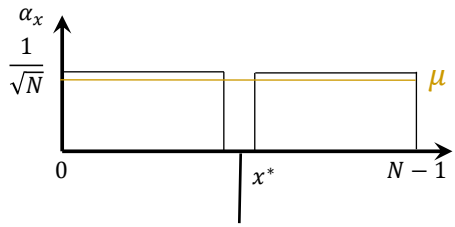
7

effetto della prima phase inversion

- alla prima phase inversion



- inoltre la media si abbassa un po'



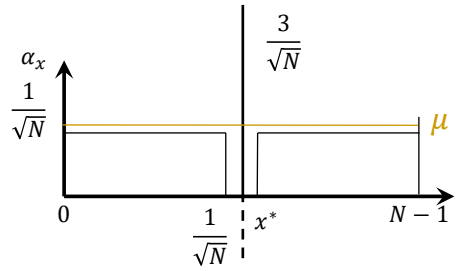
8

8

132-quantum-grover-algorithm-03

poi l'effetto della inversion about mean

- l'ampiezza di x^* viene amplificata fino a circa $\frac{3}{\sqrt{N}}$



9

9

cosa succede dopo un po'?

- intuitivamente, il valore assoluto dell'ampiezza di α_{x^*} dovrebbe crescere ad ogni iterazione
  - di quanto?
  - cosa succede dopo $\sqrt{N}$ iterazioni?
- intuitivamente passiamo da circa $\frac{3}{\sqrt{N}}$ a circa $\frac{5}{\sqrt{N}}$, ecc., con una sequenza di valori crescenti

10

10

132-quantum-grover-algorithm-03

analisi

- fissiamo l'attenzione sull'iterazione nella quale α_{x^*} arriva a circa $\frac{1}{\sqrt{2}}$
- in quella iterazione tutti gli altri valori di ampiezza $\alpha \neq \alpha_{x^*}$ sono pari a circa $\frac{1}{\sqrt{2N}}$
- infatti $(N-1)\alpha^2 = \frac{1}{2}$ e quindi $\alpha = \frac{1}{\sqrt{N-1}\sqrt{2}} \approx \frac{1}{\sqrt{2N}}$

11

11

analisi

- nel corso dell'algoritmo le ampiezze di tutti i valori diversi da x^* diminuiscono progressivamente e quindi per tutte le iterazioni nelle quali α_{x^*} è minore di $\frac{1}{\sqrt{2}}$ il loro valore è maggiore o uguale di $\frac{1}{\sqrt{2N}}$
- quindi ad ogni iterazione α_{x^*} cresce di almeno $\frac{2}{\sqrt{2N}} = \frac{\sqrt{2}}{\sqrt{N}}$, quindi per arrivare a $\frac{1}{\sqrt{2}}$ bastano $\frac{\sqrt{N}}{2}$ iterazioni e quindi $O(\sqrt{N})$ iterazioni

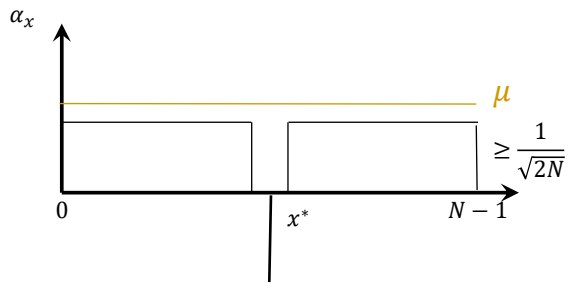
12

12

132-quantum-grover-algorithm-03

ad ogni iterazione α_{x^*} cresce di almeno

$$\frac{2}{\sqrt{2N}} = \frac{\sqrt{2}}{\sqrt{N}}$$



13

13

esercizio

- Supponi che sia $N = 4$, esegui l'algoritmo di Grover assumendo che l'elemento cercato sia in posizione 1

14

14

132-quantum-grover-algorithm-03

soluzione dell'esercizio

- abbiamo che: $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{4}} = \frac{1}{2}$
- inizializziamo: $\alpha_0 = \frac{1}{2}$, $\alpha_1 = \frac{1}{2}$, $\alpha_2 = \frac{1}{2}$, e $\alpha_3 = \frac{1}{2}$
- phase inversion: $\alpha_0 = \frac{1}{2}$, $\alpha_1 = -\frac{1}{2}$, $\alpha_2 = \frac{1}{2}$, e $\alpha_3 = \frac{1}{2}$; la media vale $\mu = \frac{3\frac{1}{2} - \frac{1}{2}}{4} = \frac{1}{4}$
- inversion about mean $(2\mu - \alpha_x)$: $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = 0$, e $\alpha_3 = 0$

15

15

implementazione della phase inversion

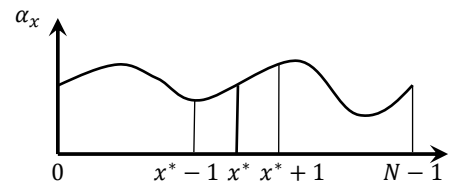
16

16

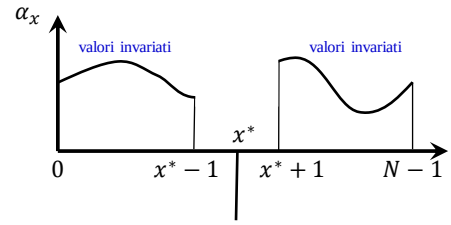
132-quantum-grover-algorithm-03

richiamo – phase inversion

- prima della phase inversion



- dopo la phase inversion



17

17

obiettivo della phase inversion

- ricordiamo il problema: è data $f:\{0,\cdots,N-1\}\rightarrow\{0,1\}$, trovare x tale che $f(x)=1$ nel caso in cui ci sia solo una x con $f(x)=1$
- se ad un certo istante il sistema si trova nello stato $\sum_x \alpha_x |x\rangle$ vogliamo portarlo nello stato $\sum_x \alpha_x (-1)^{f(x)}|x\rangle$

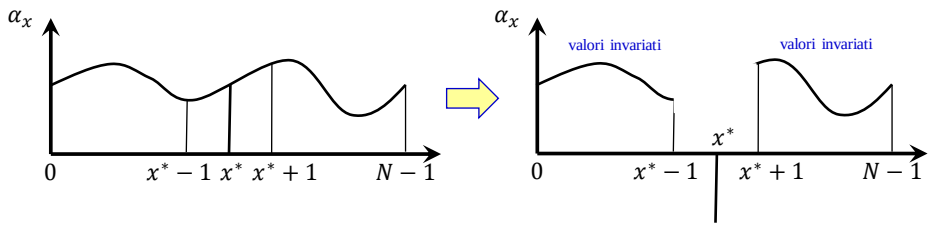
18

18

132-quantum-grover-algorithm-03

obiettivo della phase inversion

- ricordiamo il problema: è data $f:\{0,\cdots,N-1\}\rightarrow\{0,1\}$, trovare x tale che $f(x)=1$ nel caso in cui ci sia solo una x con $f(x)=1$



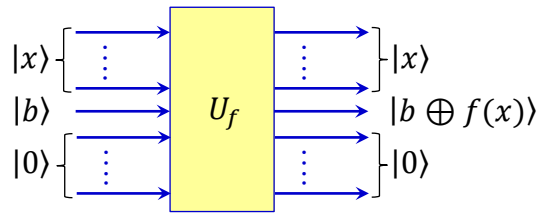
$$\sum_x \alpha_x |x\rangle \Rightarrow \sum_x \alpha_x (-1)^{f(x)} |x\rangle$$

19

19

la funzione in input

- è data come un circuito quantum



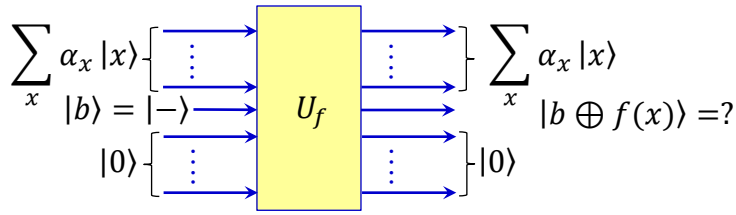
20

20

132-quantum-grover-algorithm-03

usiamo il circuito U_f

- proviamo a dare in input al posto del semplice $|x\rangle$ una superposition generica $\sum_x \alpha_x |x\rangle$ e per $|b\rangle$ usiamo lo specifico valore $|-\rangle$, cosa otteniamo?

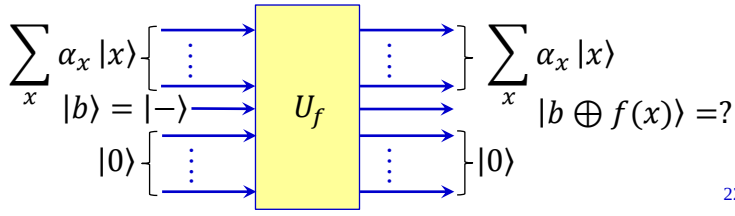


21

21

usiamo il circuito U_f

- ricordiamo che $|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$
  - se $f(x) = 0$ allora $|b \oplus f(x)\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle = |-\rangle$
  - se $f(x) = 1$ allora $|b \oplus f(x)\rangle = \frac{1}{\sqrt{2}}|1\rangle - \frac{1}{\sqrt{2}}|0\rangle = -|-\rangle$
  - quindi otteniamo in output $(-1)^{f(x)}|-\rangle$



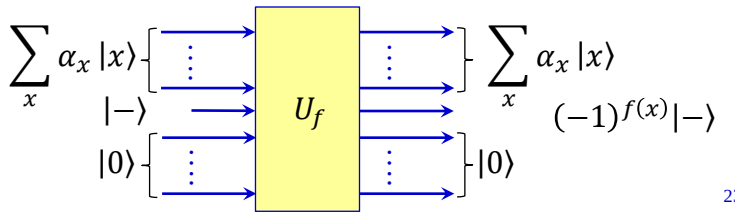
22

22

132-quantum-grover-algorithm-03

usiamo il circuito U_f

- riassumendo, abbiamo in output complessivamente $\sum_x \alpha_x |x\rangle(-1)^{f(x)}|-\rangle$

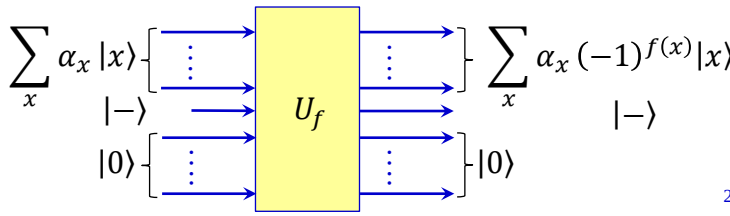


23

23

usiamo il circuito U_f

- riassumendo, abbiamo in output complessivamente $\sum_x \alpha_x |x\rangle(-1)^{f(x)}|-\rangle$
- ma questo è equivalente a $\sum_x \alpha_x (-1)^{f(x)}|x\rangle|-\rangle$
- che è ciò che volevamo



24

24

132-quantum-grover-algorithm-03

implementazione della inversion about mean

25

25

richiamo – inversion about mean

- consideriamo lo stato $\sum_x \alpha_x |x\rangle$ a un certo istante
- definiamo il valor medio μ come $\mu = \frac{\sum_{x=0}^{N-1} \alpha_x}{N}$
- inversion about mean fa il flip di ogni α_x attorno a μ, cioè trasforma ogni α_x in $2\mu - \alpha_x$
- quindi lo stato $\sum_x \alpha_x |x\rangle$ è trasformato in $\sum_x (2\mu - \alpha_x) |x\rangle$

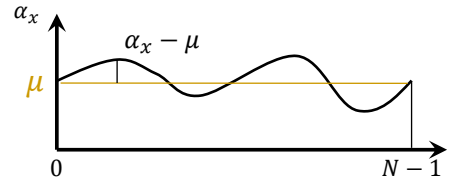
26

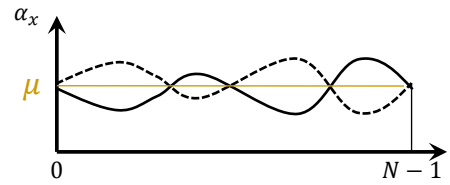
26

132-quantum-grover-algorithm-03

richiamo – inversion about mean

- osserviamo che $2\mu - \alpha_x = \mu - (\alpha_x - \mu)$ quindi, dal punto di vista grafico
- prima dell'inversion about mean
- dopo l'inversion about mean





27

27

obiettivo

- vorremmo una unitary transformation che con

input $\begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_j \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$ ottenesse in output $\begin{pmatrix} 2\mu - \alpha_0 \\ \vdots \\ 2\mu - \alpha_j \\ \vdots \\ 2\mu - \alpha_{N-1} \end{pmatrix}$

28

28

132-quantum-grover-algorithm-03

una transformation che fa per noi

- consideriamo una transformation dove tutti gli elementi hanno valore $\frac{2}{N}$ tranne quelli sulla diagonale, che hanno valore $\frac{2}{N} - 1$

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \cdots & \frac{2}{N}-1 \end{pmatrix}$$

29

29

una transformation che fa per noi

- applichiamola a un input e valutiamo l'output

$$\begin{pmatrix} \frac{2}{N}-1 & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \cdots & \cdots & \frac{2}{N}-1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \vdots \\ \alpha_j \\ \vdots \\ \alpha_{N-1} \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_j \\ \vdots \\ \beta_{N-1} \end{pmatrix}$$

- abbiamo $\beta_j = \frac{2}{N}\alpha_0 + \cdots + \left(\frac{2}{N} - 1\right)\alpha_j + \cdots + \frac{2}{N}\alpha_{N-1} = 2\frac{\sum \alpha_j}{N} - \alpha_j = 2\mu - \alpha_j$

30

30

132-quantum-grover-algorithm-03

una transformation che fa per noi

- possiamo ottenere la nostra transformation sottraendo I alla seguente matrice più semplice

$$\begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix}$$

- che si ottiene come segue

31

31

una transformation che fa per noi

- abbiamo che

$$H^{\otimes n} \begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix} H^{\otimes n} = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix}$$

- infatti ….

32

32

132-quantum-grover-algorithm-03

una transformation che fa per noi

- abbiamo che

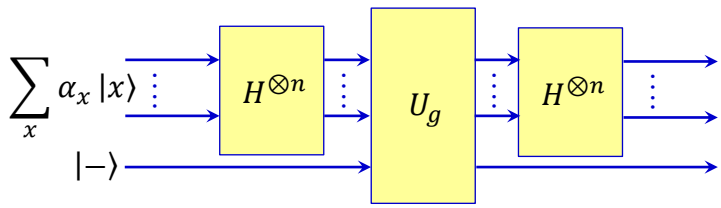
$$\begin{pmatrix} \frac{2}{\sqrt{N}} & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & 0 \\ \vdots & \vdots & & \\ \frac{2}{\sqrt{N}} & 0 & \cdots & \vdots \\ & & & 0 \end{pmatrix} H^{\otimes n} = \begin{pmatrix} \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \\ \frac{2}{N} & \ddots & \ddots & \frac{2}{N} \\ \vdots & \ddots & \ddots & \vdots \\ \frac{2}{N} & \frac{2}{N} & \cdots & \frac{2}{N} \end{pmatrix}$$

- che è ciò che ci serviva

33

33

un circuito per l'inversion about mean



dove il circuito $U_g = \begin{pmatrix} 1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ 0 & & & -1 \end{pmatrix}$, che è una unitary transformation

34

34

132-quantum-grover-algorithm-03

consideriamo i tre operatori assieme

$$H^{\otimes n}\begin{pmatrix} 1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ 0 & & & -1 \end{pmatrix}H^{\otimes n}$$

$$= H^{\otimes n}\left(\begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix} - I\right)H^{\otimes n}$$

35

35

consideriamo i tre operatori assieme

$$H^{\otimes n}\left(\begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix} - I\right)H^{\otimes n}$$

$$= H^{\otimes n}\begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}H^{\otimes n} - H^{\otimes n}IH^{\otimes n}$$

36

36

132-quantum-grover-algorithm-03

consideriamo i tre operatori assieme

$$H^{\otimes n}\begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}H^{\otimes n} - H^{\otimes n} I H^{\otimes n}$$

$$= H^{\otimes n}\begin{pmatrix} 2 & & & 0 \\ & 0 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}H^{\otimes n} - I$$

37

37

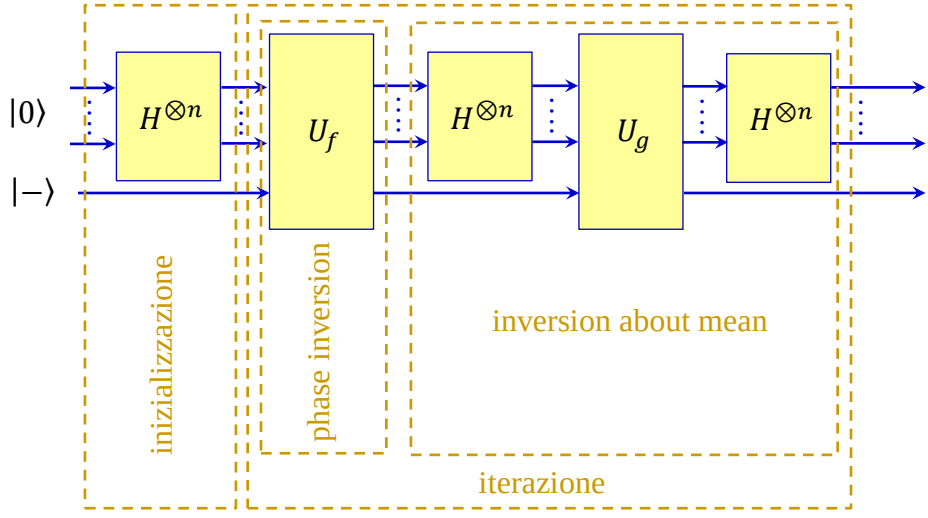
l'algoritmo di Grover

38

38

132-quantum-grover-algorithm-03

un circuito per l'algoritmo

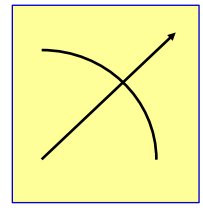


39

39

e alla fine

- non ci resta che misurare l'output



40

40