Algoritmo di Grover

Una classe estesa di problemi può essere categorizzata come **ricerca (search)**: "trova gli elementi x per cui l' affermazione $f(x)$ è vera".

Tali problemi vanno dalla ricerca in un database all'ordinamento di un database disordinato.

Un problema di ordinamento può essere rappresentato come cerca una permutazione tra due elementi per la quale è vera l'affermazione "la permutazione x porta lo stato iniziale allo stato ordinato desiderato ".

Algoritmo di Grover

Un problema di **ricerca non strutturata** è quello in cui non si sa nulla (o non si usa nessun presupposto) sulla struttura dello spazio della soluzione e la dichiarazione f. Ad esempio, determinando $f(x_0)$ non fornisce informazioni sul possibile valore di $f(x_1)$ per $x_0 \neq x_1$

Un problema di **ricerca strutturata** è quello in cui si possono trovare informazioni sulla ricerca e sull'istruzione f sfruttati. Ad esempio, la ricerca di un elenco alfabetico è un problema di ricerca strutturata e la struttura può essere sfruttata per costruire algoritmi efficienti.

Per esempio trovare un numero di telefono in una lista non ordinata di numeri di telefono con N nomi con probabilità pari a $1/2$ un algoritmo classico deve controllare un minimo di $N/2$ nomi.

In generale per una lista non ordinata, cercare a caso che sia vera una data affermazione richiede di guardare gli elementi della lista uno per uno. Quindi per una ricerca in uno spazio di dimensione N la ricerca richiede una valutazione di elementi di ordine $O(N)$.

Algoritmo di Grover

Come discusso in precedenza, un algoritmo classico per una ricerca su dati non ordinati richiede un tempo di calcolo dell'ordine di $O(N)$.

L'algoritmo di Grover esegue una ricerca su una serie non ordinata di $N = 2^n$ elementi per trovare l'elemento univoco che soddisfa una data condizione.

L'algoritmo di Grover esegue la ricerca con velocità quadratica utilizzando solo $O(\sqrt{N})$ operazioni.

Algoritmo di Grover

L'algoritmo di ricerca di Grover dimostra come le proprietà dei sistemi quantistici possano essere utilizzate per migliorare i tempi di esecuzione degli algoritmi classici. In particolare, l'algoritmo di Grover sfrutta la possibilità (solo quantistica) di:

1. sovrapposizione degli stati quantistici.
2. sfasamento dell'ampiezza degli stati quantistici.

Come altri algoritmi quantistici, l'algoritmo di Grover inizia con una **sovrapposizione uguale di tutti i possibili stati** 2^n del registro di n-qubit. Questo implica che una stessa ampiezza pari a $1/\sqrt{2^n}$ è associata ad ogni possibile configurazione di qubit nel sistema e corrisponde ad una probabilità $1/2^n$ che il sistema sia in uno di quei 2^n stati.

Algoritmo di Grover

L'algoritmo di Grover usa la cosiddetta *amplificazione di ampiezza* sfrutta cioè una proprietà caratteristica delle ampiezze quantistiche.

La proprietà utilizzata da questi algoritmi è lo sfasamento selettivo di uno stato di un sistema quantistico. Uno sfasamento di π equivale a moltiplicare l'ampiezza di quello stato per -1. Il segno dell'ampiezza per quello stato cambia, ma la probabilità di trovarsi in quello stato rimane la stessa (poiché la probabilità non dipende dal segno ma solo dall'ampiezza).

Le successive trasformazioni eseguite sul sistema sfruttano quella differenza di segno dell'ampiezza per individuare quello stato. Tale operazione non sarebbe possibile se le ampiezze non contenessero l'informazione sulla fase oltre che sulla probabilità dello stato.

Gli algoritmi ad *amplificazione di ampiezza* sono caratteristici dell'informatica quantistica grazie alla proprietà descritta delle ampiezze che non ha analoghi nel calcolo classico.

Algoritmo di Grover

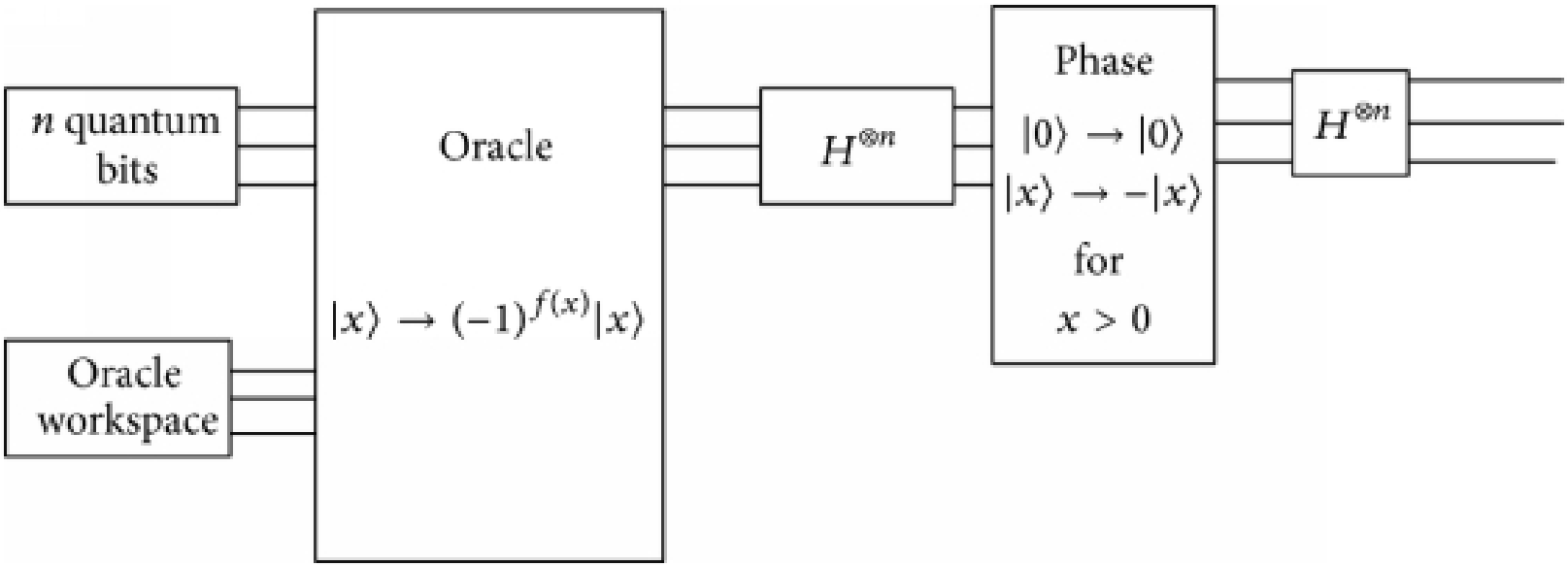
L'algoritmo di Grover inizia accedendo ad un registro quantistico di n qubit, dove n è il numero di qubit necessari per rappresentare lo spazio di ricerca della dimensione $2^n = N$ tutti inizializzati su $|0\rangle$:

$$|0\rangle^{\otimes n} = |0\rangle \tag{1}$$

Il primo passo dell'algoritmo è creare una sovrapposizione uguale di stati. Questa condizione si ottiene applicando l'operatore di Hadamard $H^{\otimes n}$ che corrisponde quindi ad n applicazioni della porta elementare di Hadamard:

$$|\psi\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \tag{2}$$

Algoritmo di Grover: Sintesi



Algoritmo di Grover

La sequenza di operazioni successive viene definita *iterazione di Grover* ed esegue l'amplificazione di ampiezza menzionata prima. Si tratta della parte centrale dell'algoritmo.

L'*iterazione di Grover* viene ripetuta $\frac{\pi}{4}\sqrt{2^n}$ volte. Secondo Grover per ottenere la massima probabilità che lo stato finale osservato sia quello giusto, la rotazione complessiva della fase deve essere $\frac{\pi}{4}$ radianti, condizione che si verifica in media dopo $\frac{\pi}{4}\sqrt{2^n}$ iterazioni.

Il primo passo dell'*iterazione di Grover* è una query quantistica (quantum oracle) $\mathcal{O}$, che modificherà il sistema a seconda che si trovi nella configurazione che stiamo cercando.

Algoritmo di Grover

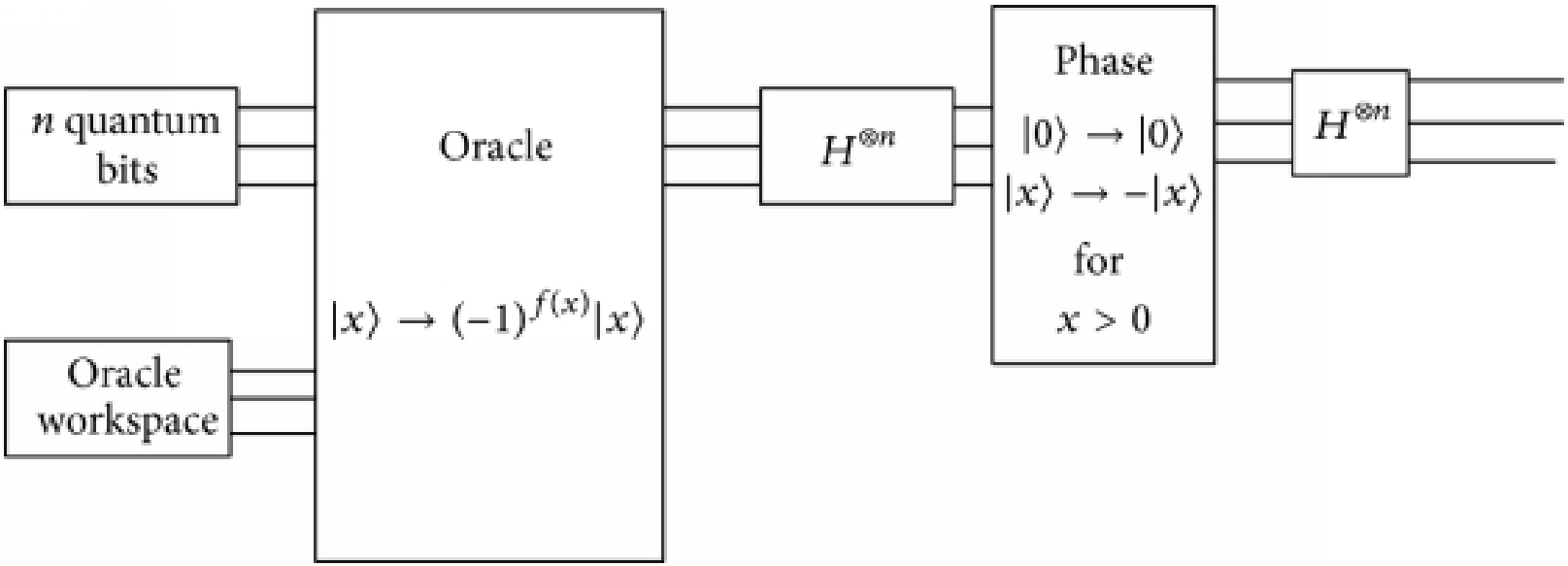
Un oracolo quantistico è una scatola nera quantistica, che può osservare e modificare il sistema senza farlo collassare nello stato classico, che riconosce se il sistema è nello stato corretto. Se il sistema si trova nello stato corretto, l'oracolo ruoterà la fase di π radianti, altrimenti non farà nulla, contrassegnando efficacemente lo stato corretto per ulteriori modifiche mediante operazioni successive. Come già menzionato in precedenza, un tale sfasamento lascia la probabilità dello stato invariata, sebbene l'ampiezza sia negata.

L'implementazione dell'oracolo quantistico, cioè il suo effetto su $|x\rangle$, può essere scritto nella forma:

$$|x\rangle \xrightarrow{\mathcal{O}} (-1)^{f(x)}|x\rangle \tag{3}$$

dove $f(x) = 1$ se x è nello stato corretto, e viceversa $f(x) = 0$. L'esatta definizione di $f(x)$ dipende dalla particolare ricerca da eseguire.

Algoritmo di Grover: Sintesi



Algoritmo di Grover

La parte successiva dell'iterazione di Grover è definita *trasformazione di diffusione*, che esegue l'inversione rispetto al valor medio, trasforma l'ampiezza di ogni stato in modo che sia al di sopra della media quanto lo era al di sotto (del valor medio) prima della trasformazione, e viceversa.

La *trasformazione di diffusione* consiste in un'altra applicazione dell'operatore di Hadamard $H^{\otimes n}$, seguita da uno sfasamento condizionale che sposta ogni stato tranne $|0\rangle$ di -1 seguito da un'ulteriore operatore di Hadamard.

Algoritmo di Grover

Lo *sfasamento condizionale* può essere rappresentato dall'operatore unitario $2|0\rangle\langle 0| - I$, che opera come segue:

$$[2|0\rangle\langle 0| - I]|0\rangle = 2|0\rangle\langle 0|0\rangle - I = |0\rangle \tag{4}$$

$$[2|0\rangle\langle 0| - I]|x\rangle = 2|0\rangle\langle 0|x\rangle - I = -|x\rangle \tag{5}$$

Complessivamente la *trasformata di diffusione*, usando il generico qubit $|\psi\rangle$ si scrive:

$$H^{\otimes n}[2|0\rangle\langle 0| - I]H^{\otimes n} = 2H^{\otimes n}|0\rangle\left\langle 0\right|H^{\otimes n} - I = 2\left|\psi\right\rangle\langle\psi| - I \tag{6}$$

Complessivamente l'iterazione di Grover si scrive includendo la query quantistica $\mathcal{O}$:

$$[2|\psi\rangle\langle\psi| - I]\mathcal{O} \tag{7}$$

Algoritmo di Grover: Sintesi

Ingresso:

- Query quantistica $\mathcal{O}$ che realizza l'operazione: $\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle$, dove $f(x) = 0$ per tutti gli $0 \leq x < 2^n$ eccetto x_0 per cui $f(x_0) = 1$.

- n qubits nello stato iniziale $|0\rangle$

Uscita: x_0

Tempo esecuzione: $O(\sqrt{2^n})$ operazioni con probabilità di riuscita $O(1)$.

Algoritmo di Grover: Sintesi

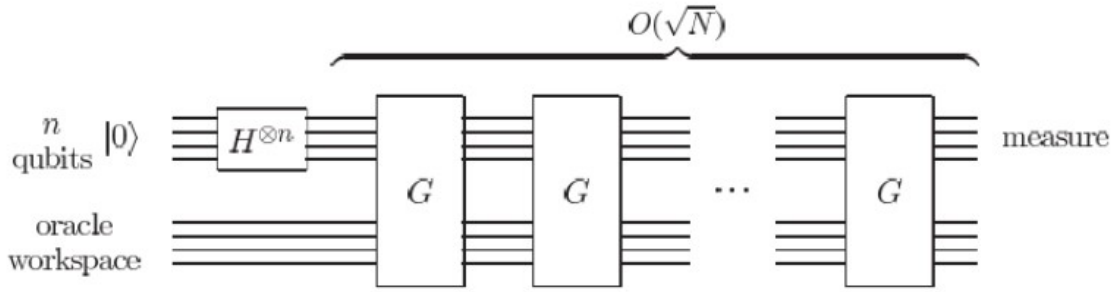


Figure 6.1. Schematic circuit for the quantum search algorithm. The oracle may employ work qubits for its implementation, but the analysis of the quantum search algorithm involves only the n qubit register.

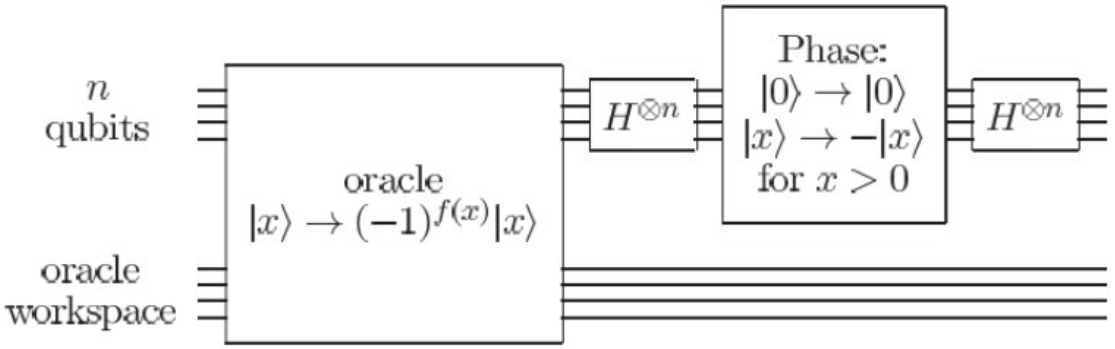


Figure 6.2. Circuit for the Grover iteration, G.

Algoritmo di Grover: Sintesi

Ingresso: - n qubits nello stato iniziale $|0\rangle$ - Query quantistica $\mathcal{O}$ che realizza l'operazione: $\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle$, dove $f(x) = 0$ per tutti gli $0 \leq x < 2^n$ eccetto x_0 per cui $f(x_0) = 1$.

Uscita: x_0

Tempo esecuzione: $O(\sqrt{2^n})$ operazioni con probabilità di riuscita $O(1)$.

Procedimento:

1. $|0\rangle^{\otimes n}$ stato iniziale

2. $H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle = |\psi\rangle$ applica l'operatore di Hadamard a tutti i qubits.

3. $[(2|\psi\rangle\langle\psi| - I)\mathcal{O}]^R|\psi\rangle \approx |x_0\rangle$ applica l'iterazione di Grover $R \approx \frac{\pi}{4}\sqrt{2^n}$ volte

4. x_0 misura il registro in uscita