Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

Lezione 14: Algoritmi quantistici di ricerca

Nel 1996 Lov Grover ha scoperto un algoritmo quantistico che permette di risolvere problemi di ricerca non strutturati fornendo un miglioramento quadratico rispetto alle prestazioni dei relativi algoritmi classici.

1 Problemi di ricerca

I problemi di ricerca costituiscono una numerosa classe di problemi che vanno dalla ricerca in una base di dati all'ordinamento e alla colorazione di un grafo. La forma generale di un problema di ricerca é: "trovare un elemento x in un insieme di possibili soluzioni tale che una certa condizione $P(x)$ é vera". Per esempio, il problema della colorazione di un grafo si puó vedere come la ricerca di un assegnamento di colori ai vertici tale che la condizione "vertici adiacenti hanno colori diversi" é soddisfatta. Analogamente un problema di ordinamento equivale alla ricerca di una permutazione che soddisfa la particolare relazione d'ordine desiderata.

Un problema di ricerca non strutturato é un problema di ricerca dove non si conosce ne' la struttura dello spazio delle soluzioni, ne' la condizione P. Per un problema di ricerca strutturato queste informazioni possono invece essere uitilizzate permettendo di costruire algoritmi efficienti (e.g. ricerca binaria per problemi di ricerca dove lo spazio delle soluzioni ha una struttura di albero binario).

Nel caso generale di un problema di ricerca non strutturato, il migliore algoritmo classico che si possa applicare é quello che controlla la condizione $P(x)$ su ciascuno degli elementi scelti casualmente nell'insieme delle possibili soluzioni. Se quest'ultimo ha dimensione N, allora l'algoritmo richiede $O(N)$ valutazioni di P. Tuttavia, su un computer quantistico, questi problemi si posssono risolvere con una probabilitá di errore limitata, con $O(\sqrt{N})$ valutazioni di P, utilizzando il metodo di Grover che descriviamo nel seguito.

Questo metodo é stato dimostrato ottimale per problemi di ricerca completamente non strutturati e la sue applicazioni piú importanti e utili sono per ottenere soluzioni piú rapide per problemi **NP**-hard.

2 L'algoritmo di Grover

Assumiamo per convenienza che il numero di possibili soluzioni del problema di ricerca sia $N = 2^n$ e che ogni elemento sia una una sequenza di n bits. Assumiamo inoltre che il numero delle soluzioni sia esattamente M e che esista un oracolo che determina se una data sequenza di n bits é una soluzione oppure no. Tale oracolo corrisponde ad una trasformazione unitaria che implementa una particolare funzione booleana $f : \{0,1\}^n \mapsto \{0,1\}$ tale che $f(x) = 1$ se x é una soluzione e $f(x) = 0$ altrimenti, e ha la forma:

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

dove $x \in \{0,1\}^n$ e $|q\rangle$ é un singolo qubit. Se inizializzato a 0, q diventa 1 quando $f(x) = 1$. Se $|q\rangle$ é preparato nello stato $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, allora l'azione dell'oracolo O é quella di invertire le ampiezze degli stati $|x\rangle$ che sono soluzioni, lasciando invariati gli altri stati:

$$O : |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}} \mapsto (-1)^{f(x)} |x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$

Poiché il qubit $|q\rangle$ non viene modificato da O possiamo ignorarlo. L'azione di O su un generico stato quantistico é quindi:

$$O : \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle \mapsto \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \alpha_x |x\rangle .$$

L'algoritmo di Grover é definito su un input preparato nello stato $|0\rangle^{\otimes n}$. Viene quindi applicata la trasformata di Hadamard per ottenere la sovrapposizione equiprobabile di stati

$$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x\in\{0,1\}^n} |x\rangle .$$

A questo punto si ripete l'applicazione per un numero appropriato di volte del seguente operatore, detto operatore di Grover,

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

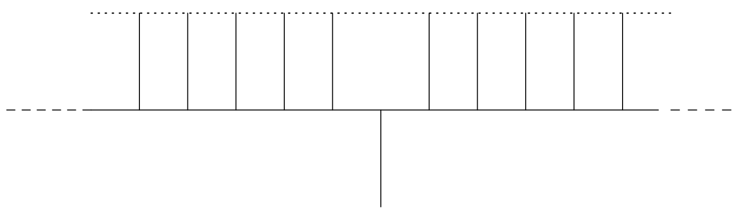

Figure 1: Effetto dell'oracolo O sulle ampiezze

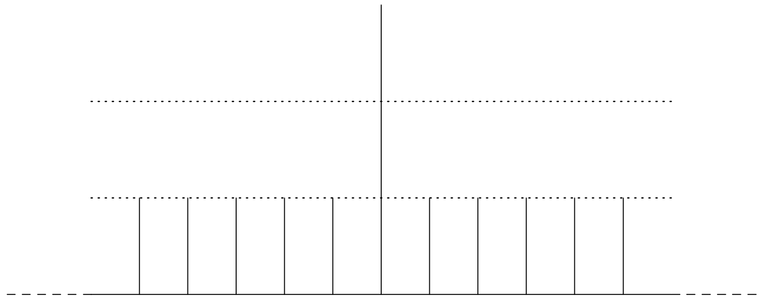

Figure 2: Inversione intorno alla media delle ampiezze

dove P_0 effettua uno shift di fase di -1 su tutti gli stati computazionali diversi da $|0\rangle$, cioé

$$P_0 : |x\rangle \mapsto \begin{cases} |x\rangle & \text{se } x = 0 \\ -|x\rangle & \text{se } x > 0 \end{cases},$$

per ogni $0 \leq x \leq N-1$. Si verifica facilmente che $P_0 = 2|0\rangle\langle 0| - I$.

L'operazione $H^{\otimes n} P_0 H^{\otimes n}$ é detta "inversione intorno alla media" perché il suo effetto é quello di amplificare le ampiezze degli stati soluzione (che erano state moltiplicate per -1 dall'oracolo, cf. Figura 1) innalzandole del doppio al di sopra della media di tutte le ampiezze (cf. Figura 2).

Formalmente tale operazione corrisponde a

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

e la sua azione su un generico stato $\sum_x \alpha_x |x\rangle$ é

$$(2|\psi\rangle\langle\psi| - I)(\sum_x \alpha_x |x\rangle) = \sum_x (2A - \alpha_x)|x\rangle,$$

dove $A = \sum_x \alpha_x / N$. La dimostrazione segue dall'osservazione che la matrice

$N \times N$ definita da:

$$D = \begin{bmatrix} \frac{2}{N} - 1 & \frac{2}{N} & \dots & \frac{2}{N} \\ \frac{2}{N} & \frac{2}{N} - 1 & \dots & \frac{2}{N} \\ \dots & \dots & \dots & \dots \\ \frac{2}{N} & \frac{2}{N} & \dots & \frac{2}{N} - 1 \end{bmatrix}$$

é unitaria ed effettua la trasformazione $\sum_x \alpha_x |x\rangle) \mapsto \sum_x (2A - \alpha_x) |x\rangle$. Questa matrice corrisponde esattamente a $H^{\otimes n}(2|0\rangle\langle 0|)H^{\otimes n} - I$. Infatti

$$H^{\otimes n}(2|0\rangle\langle 0|)H^{\otimes n} = \frac{2}{N} \sum_{x,y} |x\rangle\langle y| = \begin{bmatrix} \frac{2}{N} & \dots & \frac{2}{N} \\ \dots & \frac{2}{N} & \dots \\ \frac{2}{N} & \dots & \frac{2}{N} \end{bmatrix}.$$

Possiamo quindi scrivere l'operatore di Grover come

$$G = (2|\psi\rangle\langle\psi| - I)O.$$

2.1 Interpretazione geometrica di G

L'operatore di Grover corrisponde ad una rotazione dello stato iniziale $|\psi\rangle$ nel piano reale generato dai due stati normalizzati

$$|\sigma\rangle = \frac{1}{\sqrt{N-M}} \sum_{x \in S} |x\rangle \text{ e } |\tau\rangle = \frac{1}{\sqrt{M}} \sum_{x \in T} |x\rangle ,$$

dove $T = \{x \in \{0,1\}^n \mid f(x) = 1\}$ e $S = \{0,1\}^n \setminus T$. Questi due stati corrispondono a sovrapposizioni uniformi rispettivamente degli stati che non sono soluzioni e di quelli che sono soluzioni. Si verifica facilmente che $|\psi\rangle$ appartiene al piano generato da $|\sigma\rangle$ e $|\tau\rangle$, cioé che

$$|\psi\rangle = \sqrt{\frac{N-M}{N}} |\sigma\rangle + \sqrt{\frac{M}{N}} |\tau\rangle .$$

Per vedere che G é una rotazione, osserviamo che l'azione dell'oracolo O in questo piano é una riflessione intorno all'asse $|\sigma\rangle$. Infatti, per ogni stato nel piano, $a|\sigma\rangle + b|\tau\rangle$ (con $a^2 + b^2 = 1$), $O(a|\sigma\rangle + b|\tau\rangle) = a|\sigma\rangle - b|\tau\rangle$.

Esercizio 2.1 *Dimostra che l'azione di* $2|\psi\rangle\langle\psi| - I$ *nel piano* $|\sigma\rangle$, $|\tau\rangle$ *é una riflessione intorno a* $|\psi\rangle$.

Pertanto G é la composizione di due riflessioni e il seguente teorema della geometria piana ci assicura che questa composizione corrisponde ad una rotazione.

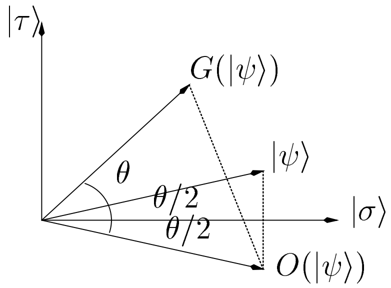

Figure 3: Singola iterazione dell'operatore G

Teorema 2.2 *Se L_1 e L_2 sono due rette nel piano euclideo $\mathbb{R}^2$ che si intersecano in un punto P, e se β é l'angolo tra L_1 e L_2, allora una riflessione in L_1 seguita da una riflessione in L_2 é una rotazione di un angolo 2β intorno al punto P.*

Allora, se $\theta/2$ é l'angolo tra $|\psi\rangle$ e $|\sigma\rangle$ (cf. Figura 3), l'operatore G ruota i vettori nel piano $|\sigma\rangle, |\tau\rangle$ di un angolo θ verso $|\tau\rangle$. Poiché $|\psi\rangle = \cos\theta/2\,|\sigma\rangle + \sin\theta/2\,|\tau\rangle$, l'angolo $\theta/2$ é tale che $\cos\theta/2 = \sqrt{(N-M)/N}$ e $\sin\theta/2 = \sqrt{M/N}$.

Esercizio 2.3 *Dimostrare che nella base $|\sigma\rangle, |\tau\rangle$ l'operatore G ha la matrice di rappresentazione*

$$\begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix},$$

dove θ é un numero reale in $[0, \pi/2]$ tale che $\sin\theta/2 = \sqrt{M/N}$. (Nota che $\sin\theta = \sin 2\theta/2 = 2\sin\theta/2\cos\theta/2 = \frac{2\sqrt{M(N-M)}}{N}$).

Dopo m iterazioni abbiamo:

$$G^m\,|\psi\rangle = \cos\,(\frac{2m+1}{2}\theta)\,|\sigma\rangle + \sin\,(\frac{2m+1}{2}\theta)\,|\tau\rangle\,.$$

Se $\frac{2m+1}{2}\theta) \approx \pi/2$, cioé dopo

$$m = int(\pi/2\theta - 1/2)$$

iterazioni (dove $int(x)$ denota la parte intera del numero reale x), l'angolo tra $|\psi\rangle$ e $|\sigma\rangle$ é $\pi/4$, che é quindi uguale all'angolo tra $|\psi\rangle$ e $|\tau\rangle$, poiché i due angoli sono complementari. Quindi una misurazione di $|\psi\rangle$ ci darebbe una soluzione con probabilitá $\sin^2\pi/4 = 1/2$.

In generale, dall'equazione precedente segue che $m \leq up(\pi/2\theta)$ (dove $up(x)$ denota la parte intera alta di x). Poiché per ogni $\theta \in \mathbb{R}$

$$\frac{\theta}{2} \geq \sin\frac{\theta}{2} = \sqrt{\frac{M}{N}},$$

si ottiene il seguente limite superiore per il numero di iterazioni di G necessarie per trovare una soluzione:

$$m \leq up\left(\frac{\pi}{4}\sqrt{\frac{N}{M}}\right).$$

2.2 Complessitá

La complessitá dell'algoritmo di Grover é data essenzialmente dal numero m di iterazioni dell'operatore G che, come abbiamo visto precedentemente, é $O\left(\sqrt{\frac{N}{M}}\right)$. In ogni iterazione viene applicata due volte la trasformata di Hadamard che richiede $O(n) = O(\log N)$ operazioni su un singolo qubit. Quindi complessivamente l'algoritmo di Grover ha un costo computazionale di $O\left(\sqrt{\frac{N}{M}}\log N\right)$.