One-Way Quantum Computer

June 26, 2009

Esistono vari modelli di computazione quantistica che risultano equivalenti dal punto di vista formale, cioè in grado di implementare gli stessi algoritmi quantistici, ma che risultano profondamente diversi nei loro concetti di base e, cosa ancora più importante, nei requisiti per la loro realizzazione pratica.
Analizzeremo qui il modello di *measurement-based quantum computation* dove l'informazione quantistica viene processata tramite misure di qubit preparati in stati entangled. In particolare analizzeremo il modello di *one-way quantum computation* dove tutto l'entanglement necessario alla computazione viene fornito all'inizio tramite un particolare stato entangled, lo *stato cluster*, composto da un grande numero di qubit. Successivamente l'informazione viene scritta, processata e letta tramite misure di singoli qubit. Lo stato di cluster fornisce quindi un "substrato universale" per ogni computazione quantistica.
Un modo per creare questi stati cluster è quello di utilizzare un reticolo a 2 o 3 dimensioni di particelle a due stati quantistici con un'interazione di tipo Ising a temperatura molto bassa. Consideriamo l'interazione di Ising tra primi vicini descritta dall'hamiltoniana:

$$H_{int} = -\frac{1}{4} g(t) \sum_{\langle a,a' \rangle} \sigma_z^{(a)} \sigma_z^{(a')} \tag{1}$$

dove la somma è intesa tra i primi vicini e $g(t)$ è un parametro controllabile esternamente da cui dipende la forza dell'interazione. Un qubit in un sito (a) può stare in una sovrapposizione $\alpha|0\rangle_a + \beta|1\rangle_a$ con $|\alpha|^2 + |\beta|^2 = 1$ dove $|0\rangle_a \equiv |0\rangle_{z,a}$ e $|1\rangle_{z,a}$ sono gli autostati dell'operatore di Pauli $\sigma_z^{(a)}$ al sito a.
La preparazione dello stato cluster avviene in questo modo: si preparano tutti i qubit nello stato $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, l'autostato dell'operatore σ_x, poi si accende l'interazione H_{int} tramite il parametro di controllo $g(t)$ per un tempo T tale che $\int_0^T g(t)dt = \pi$. L'evoluzione temporale genera una trasformazione unitaria S sul sistema che, dato che H_{int} agisce in modo uniforme, genera uno stato entangled di tutto il sistema in una volta sola. Chiamiamo C il cluster e $|\Phi\rangle_C$ lo stato entangled così ottenuto, si può dimostrare [1] che soddisfa un insieme di equazioni agli autovalori:

$$\sigma_x^{(a)} \bigotimes_{a' \in ngbh(a)} \sigma_z^{(a')} |\Phi\rangle_C = \pm |\Phi\rangle_C \tag{2}$$

dove $ngbh(a)$ specifica i siti a' che interagiscono col sito a e gli autovalori dipendono dalla distribuzione di qubit nel reticolo. Questo set di equazioni è fondamentale per poter svolgere la computazione tramite misure di singolo qubit.

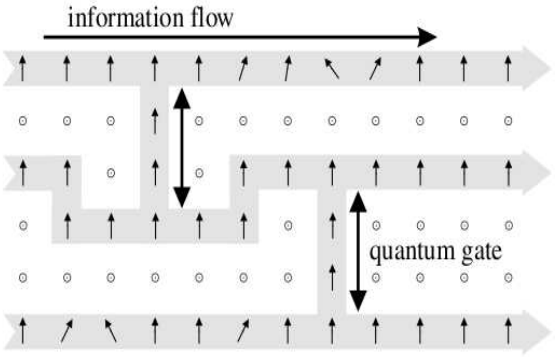

Figure 1:

Infatti, nonostante il risultato della singola misura è indeterminato, possiamo proiettare due qubit a, a' in uno stato di Bell tramite misure su un sottinsieme degli altri qubit e successivamente implementare porte logiche a meno di rotazioni finali che dipenderanno dai risultati delle misure effettuate.
Vedremo che il cluster è come uno strato su cui "stampare il circuito quantistico" tramite misure di singolo qubit. Possiamo farci un'idea di questo considerando la fig.1.

Come primo passo della computazione si crea un "network" (regione scura in figura), tramite misure di σ_z sul resto del cluster, che di fatto elimina questi qubit (cioè li proietta in stati non entangled). Lo stato $|\Phi\rangle_C$ viene proiettato nello stato $|\mu\rangle_{C\setminus\mathcal{N}} \otimes |\tilde{\Phi}\rangle_{\mathcal{N}}$, dove $|\mu\rangle_{C\setminus\mathcal{N}}$ è lo stato delle particelle misurate ($C\setminus\mathcal{N}$), mentre $|\tilde{\Phi}\rangle_{\mathcal{N}}$ è lo stato entangled delle particelle non ancora misurate ($\mathcal{N} \subset C$). Lo stato $|\tilde{\Phi}\rangle_{\mathcal{N}}$ è legato allo stato $|\Phi\rangle\_mathcalN$ da una trasformazione unitaria che dipende dai risultati delle misure effettuate, e in particolare soddisfa un set di equazioni simile a (2) a parte una eventuale differenza di segno dipendente dai risultati delle misure.
Una volta ottenuto il network l'informazione viene processata effettuando misure di singolo qubit in un certo ordine e in una certa base. L'informazione quantistica viene fatta viaggiare in "orizzontale" attraverso il cluster effettuando misure lungo le linee mentre le connessioni verticali realizzano le porte logiche a due qubit. La base in cui vengono effettuate le misure dipenderà dai risultati delle misure precedenti. Il processamento dell'informazione finisce quando tutti i qubit, eccetto l'ultimo di ogni linea, sono stati misurati, a questo punto per leggere l'"output" si deve effettuare la misura in una certa base dipendente dai risultati delle misure precedenti. Osserviamo che durante tutto il processo utilizziamo solo misure a un qubit quindi l'entanglement diminuisce ad ogni passaggio.
Vedremo ora che ogni circuito logico quantistico può essere implementato su uno stato cluster (purchè ovviamente abbastanza grande), in questo modo oltre ad avere una dimostrazione di universalità illustreremo come si realizzano particolari circuiti quantistici. Per semplicità partiamo con questo schema:1) scegliamo alcuni qubit come qubit di input e scriviamo l'input su questi, 2) prepariamo tutti gli altri nello stato $|+\rangle$, 3) procediamo con l'operazione di entanglement S

per creare lo stato cluster, 4) "stampiamo" il circuito quantistico e effettuiamo la computazione. Vedremo alla fine (punto (e))che l'operazione 1) non è necessaria, l'input può essere inserito durante l'operazione 4).
Vediamo ora quali sono gli elementi di base di un circuito quantistico e come si possono comporre:

(a) *Propagazione dell'informazione lungo le linee.* Consideriamo una catena di un numero dispari di qubit $1, \ldots, n$ preparati nello stato $|\psi_{in}\rangle_1 \otimes |+\rangle_2 \otimes \ldots \otimes \|+\rangle_n$ e successivamente portati in uno stato entangled dall'evoluzione S. Lo stato $|\psi_{in}\rangle$ originariamente registrato nel qubit 1 può essere trasferito al sito n tramite misure di σ_x , cioè nella base $\{|+\rangle_j \equiv |0\rangle_{x,j}, |-\rangle_j \equiv |1\rangle_{x,j}\}$, sui siti $j = 1, \ldots, n-1$ che danno come risultati $s_j \in \{0, 1\}$. A questo punto lo stato risultante sarà $|s_1\rangle_{x,1} \otimes \ldots \otimes |s_{n-1}\rangle_{x,n-1} \otimes |\psi_{out}\rangle_n$. L'output $|\psi_{out}\rangle$ è legato all'input $|\psi_{in}\rangle$ da una trasformazione unitaria $U_\Sigma \in \{1, \sigma_x, \sigma_z, \sigma_x\sigma_z\}$ che dipende dai risultati delle misure di σ_x.
Nel caso di un numero pari di qubit si può fare un ragionamento analogo.
Osserviamo inoltre che per tale scelta bastano due bit classici, non è quindi necessario registrare tutti i risultati delle misure ma solo due bit che andranno aggiornati ad ogni misura.

(b) *Rotazione arbitraria $U_R \in SU(2)$.* Scriviamo la rotazione U_R nella rappresentazione di Eulero $U_R[\xi, \eta, \zeta] = U_x(\zeta)U_z(\eta)U_x(\xi)$ dove
$U_{x,z}(\alpha) = \exp(-i\alpha\frac{\sigma_{x,z}}{2})$. Consideriamo una catena di cinque qubit e supponiamo di voler ruotare il primo che è nello stato $|\psi_{in}\rangle$, mentre gli altri sono nello stato $|+\rangle$. Lo stato della catena sarà quindi $|\Psi\rangle_{1,\ldots,5} = |\psi_{in}\rangle_1 \otimes |+\rangle_2 \otimes |+\rangle_3 \otimes |+\rangle_4 \otimes |+\rangle_5$. Dopo la trasformazione S si troveranno nello stato $S|\Psi\rangle_{1,\ldots,5} = 1/2|\psi_{in}\rangle_1 \otimes |0\rangle_2 \otimes |-\rangle_3 \otimes |0\rangle_4 \otimes |-\rangle_5 - 1/2|\psi_{in}\rangle_1 \otimes |0\rangle_2 \otimes |+\rangle_3 \otimes |1\rangle_4 \otimes |+\rangle_5 - 1/2|\psi^*_{in}\rangle_1 \otimes |1\rangle_2 \otimes |+\rangle_3 \otimes |0\rangle_4 \otimes |-\rangle_5 + 1/2|\psi^*_{in}\rangle_1 \otimes |1\rangle_2 \otimes |-\rangle_3 \otimes |1\rangle_4 \otimes |+\rangle_5$, dove $|\psi^*_{in}\rangle = \sigma_z|\psi_{in}\rangle$. Ora possiamo ruotatare lo stato $|\psi_{in}\rangle$ e insieme trasportarlo sul qubit 5 misurando i qubit $1, \ldots, 4$ nella base $\mathcal{B}_j(\alpha_j) = \{\frac{|0\rangle_j + e^{i\alpha_j}|1\rangle_j}{\sqrt{2}}, \frac{|0\rangle_j - e^{i\alpha_j}|1\rangle_j}{\sqrt{2}}\}$ con certi risultati $s_j \in \{0, 1\}$. Lo stato finale sarà quindi $|s_1\rangle_{\alpha_1,1} \otimes |s_2\rangle_{\alpha_2,2} \otimes |s_3\rangle_{\alpha_3,3} \otimes |s_4\rangle_{\alpha_4,4} \otimes |\psi_{out}\rangle_5$, con $|\psi_{out}\rangle = U|\psi_{in}\rangle$ e U una certa trasformazione unitaria. Si può dimostrare che per la scelta di $\alpha_1 = 0$ la trasformazione U ha la forma
$U = \sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}U_R[(-1)^{s_1+1}\alpha_2, (-1)^{s_2}\alpha_3, (-1)^{s_1+s_3}\alpha_4]$. Si può quindi implementare una rotazione $U_R[\xi, \eta, \zeta]$ arbitraria effettuando misure successive nelle basi $\mathcal{B}_1(0)$, $\mathcal{B}_2((-1)^{s_1+1}\xi), \mathcal{B}_3((-1)^{s_2}\eta), \mathcal{B}_4((-1)^{s_1+s_3}\zeta)$, in questo modo si ottiene la rotazione voluta a meno di una ulteriore rotazione $\sigma_x^{s_2+s_4}\sigma_z^{s_1+s_3}$ di cui si può tener conto alla fine della computazione (punto (d)).

(c) *Porta `CNOT`.* Vogliamo costruire una porta `CNOT` in cui il qubit di target viene trasferito dal sito t_{in} al sito t_{out}, per fare questo abbiamo bisogno di quattro qubit disposti secondo la figura $2(a)$.
Sia 1 il qubit di target iniziale e 4 il qubit di controllo e 3 il qubit di target finale. Prepariamo lo stato $|i_1\rangle_{z,1} \otimes |i_4\rangle_{z,4} \otimes |+\rangle_2 \otimes |+\rangle_3$ e applichiamo la trasformazione S. Misurando σ_x sui qubit 1 e 2 con risultati $s_j \in \{0, 1\}$ otteniamo lo stato $|s_1\rangle_{x,1} \otimes |s_2\rangle_{x,2} \otimes U_\Sigma^{(34)}|i_4\rangle_{z,4} \otimes |i_1 + i_4 mod 2\rangle_{z,3}$, dove $U_\Sigma^{(34)} = \sigma_z^{(3)^{s_1+1}}\sigma_x^{(3)^{s_2}}\sigma_z^{(4)^{s_1}}$.
Otteniamo quindi una porta `CNOT` più una rotazione non voluta di cui,come vedremo, si può tener conto alla fine della computazione come per il caso pre-

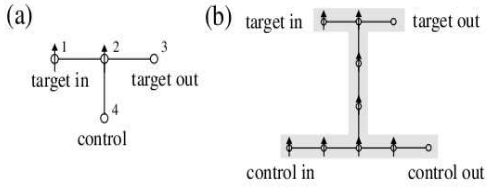

Figure 2:

cendente. In realtà quando la porta `CNOT` deve essere usata insieme ad altre porte per formare un circutio quantistico è più opportuno utilizzarla nella forma mostrata in figura (2b).

(d) *Circuiti quantistici.* Abbiamo mostrato che tramite uno stato cluster e tutte le misure a un singolo qubit possiamo ottenere la porta `CNOT` e una rotazione arbitraria di ogni qubit, abbiamo quindi un set universale di porte quantistiche.
Nell'implementazione di un circuito quantistico ogni sito di output di una porta quantistica corrisponde al sito di input della porta successiva, vediamo ora che tutta l'operazione di entanglement può essere effettuata in una volta sola all'inizio della computazione.
Per capire meglio questa idea consideriamo un network $\mathcal{N}$ di qubit diviso in due circuiti consecutivi 1 e 2 implementati da due network $\mathcal{N}_1$ e $\mathcal{N}_2$, cioè $\mathcal{N} = \mathcal{N}_1 \cup \mathcal{N}_2$, con un insieme $\mathcal{O} = \mathcal{N}_1 \cap \mathcal{N}_2$ che è l'output del primo ed anche l'input del secondo, e un insieme $\mathcal{R}$ che contiene l'output del secondo.
Supponiamo di adottare la seguente strategia:1) scriviamo l'input e creiamo stato entangled sul network $\mathcal{N}_1$; 2) misuriamo i qubit su $\mathcal{N}_1 \setminus \mathcal{O}$ questo implementa il circuito su $\mathcal{N}_1$ e scrive l'output intermedio su $\mathcal{O}$; 3) creiamo lo stato entangled su $\mathcal{N}_2$; 4) misuriamo i qubit su $\mathcal{N}_2 \setminus \mathcal{R}$. I punti $3), 4)$ implementano il circuito 2 su $\mathcal{N}_2$, ma, dato che le operazioni di misura su $\mathcal{N}_1$ descritte al punto 2) commutano con le operazioni di entanglement e di misura ai punti $3), 4)$, possiamo portare direttamente tutto il cluster in una volta sola nello stato entangled.
Dobbiamo ancora affrontare il problema delle rotazioni extra necessarie per implementare le rotazioni U_R e la porta `CNOT`. Utilizzando le relazioni
$U_R(\xi,\eta,\zeta)\sigma_z^s\sigma_x^{s'} = \sigma_z^s\sigma_x^{s'}U_R((-1)^s\xi,(-1)^{s'}\eta,(-1)^s\zeta)$ e
$\texttt{CNOT}(c,t)\sigma_z^{(t)^{s_t}}\sigma_z^{(c)^{s_c}}\sigma_x^{(t)^{s_t'}}\sigma_x^{(c)^{s_c'}} = \sigma_z^{(t)^{s_t}}\sigma_z^{(c)^{s_c+s_t}}\sigma_x^{(t)^{s_t'+s_c'}}\sigma_x^{(c)^{s_c'}}\texttt{CNOT}(c,t)$
possiamo "trasferire" queste rotazioni attraverso il network all'output finale e tenerne conto modificando la base in cui facciamo la misura per ottenere la lettura dell'output.

(e) *Schema completo* Rimane da affrontare il problema della scrittura dell'input iniziale. Per semplicità di esposizione abbiamo assunto che venisse scritto prima dell'operazione di entanglement S ma ora possiamo dimostrare che non è necessario. Consideriamo una catena di cinque qubit preparati nello stato $S|+\rangle_1 \otimes |+\rangle_2 \otimes |+\rangle_3 \otimes |+\rangle_4 \otimes |+\rangle_5$, dal punto (b) sappiamo che possiamo proiettare il qubit 5 in un qualsiasi stato (a meno di una rotazione U_Σ) utilizzando solo il

fatto che il quibit 1 è nello stato $|+\rangle_1$. A questo punto il qubit 5 è nello stato desiderato e può essere usato per la successiva computazione poichè è ancora in uno stato entangled con il resto del network.

Per concludere possiamo dire che lo stato cluster in cui il sistema viene inizializzato contiene tutte le risorse necessarie per la computazione, indipendentemente dall'algoritmo che si vuole implementare, si definisce quindi "risorsa universale". Questo in particolare implica che la potenza di calcolo di un computer quantistico costruito in questo modo dipende solamente dalle proprietà dello stato cluster a disposizione. Inoltre il problema della realizzazione sperimentale si riduce al problema di preparare uno specifico stato entangled e al problema di compiere misure sui singoli qubit. Infine citiamo due possibili realizzazioni pratiche: stato cluster di atomi neutri a bassa temperatura intrappolati in un reticolo ottico, stato cluster realizzato con fotoni. Il primo approccio offre la possibilità di ottenere stati cluster su larga scala con alta efficienza, ci sono però difficoltà nel compiere misure sui singoli siti. Viceversa i fotoni permettono di compiere operazioni sui singoli qubit con grande precisione, ma rendono difficile costruire cluster su larga scala.

References

[1] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 910 (2001).

[2] H.-J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86**, 5188 (2001).

[3] H. J. Briegel, D. E. Browne, W. Duer, R. Raussendorf and M. Van den Nest, Nature Physics **5**, 19 (2009).