Classical simulation of quantum circuits

Laureando: Tommaso Gagliardoni
Relatore: Prof. Marco Baioletti

Università degli Studi di Perugia
Corso di Laurea Specialistica in Matematica - Curriculum Informatico-Computazionale

27 Maggio 2011, Perugia

Introduzione - Il computer quantistico

Computer quantistico: dispositivo di calcolo che basa il suo funzionamento sulle leggi della meccanica quantistica.

Timeline essenziale:

- 1981: primo modello teorico di QC (R. Feynman)
- 1994: algoritmo di Shor
- 1996: algoritmo di Grover
- 1998: realizzazione di un QC a 3 qubit
- 2000: realizzazione di un QC a 7 qubit
- 2001: fattorizzazione del numero 15
- 2006: realizzazione di un QC a 12 qubit
- 2008: realizzazione di un QC adiabatico a 128 qubit

Introduzione - Potenzialità del computer quantistico

Computer classico: dati binari 0 o 1.

Computer quantistico: principio di *sovrapposizione* (molto controintuitivo, pochi problemi studiati, difficile estrarre i dati).

Per alcuni problemi che hanno una struttura molto particolare, il computer quantistico è in grado di superare le performances di un computer classico.

Esempio: algoritmo di Shor: fattorizzazione di numeri interi di lunghezza n in tempo polinomiale invece che subesponenaziale.

Meccanica quantistica

Postulato 1: sistema fisico $\leftrightsquigarrow$ spazio di Hilbert complesso $\mathcal{H}$.

Bra-ket notation:

- vettore $|\psi\rangle \in \mathcal{H}$
- prodotto interno tra $|\psi\rangle$ e $|\phi\rangle$: $\langle\psi|\phi\rangle$
- duale di un vettore: $\langle\phi| \in \mathcal{H}', \langle\phi| : |\psi\rangle \mapsto \langle\phi|\psi\rangle$

Stato di un sistema: classe di equivalenza di vettori normalizzati:

$$|\langle\psi|\psi\rangle|^2 = |\langle\phi|\phi\rangle|^2 = 1; |\psi\rangle \sim |\phi\rangle \iff |\psi\rangle = \lambda\,|\phi\rangle\,, |\lambda| = 1$$

Sistema fisico elementare: qubit (spazio dimensione 2, base $|0\rangle$ e $|1\rangle$).

Meccanica quantistica

Postulato 2: sistema fisico composto $\leftrightsquigarrow$ prodotto tensore tra relativi spazi di Hilbert dei componenti.

Esempio: sistema fisico A rappresentato da $\mathcal{H}$, sistema fisico B rappresentato da $\mathcal{J}$. Il sistema fisico $A \cup B$ (che prende in esame A e B contemporaneamente) sarà rappresentato da $\mathcal{H} \otimes \mathcal{J}$.

Esempio: sistema di n qubit $\leftrightsquigarrow$ spazio di Hilbert 2^n-dimensionale.

Base:

$$|0\ldots00\rangle \ , \ |0\ldots01\rangle \ , \ |0\ldots10\rangle \ , \ \ldots \ , \ |1\ldots11\rangle$$

Meccanica quantistica

Postulato 3: osservabile di un sistema $\leftrightsquigarrow$ operatore Hermitiano $A = A^\dagger : \mathcal{H} \to \mathcal{H}$.

Autovalori: $\lambda_1, \ldots, \lambda_d$ (reali).
Base ortonormale di autovettori (autostati): $|\gamma\rangle_1, \ldots, |\gamma\rangle_d$

Misura dell'osservabile A su uno stato $|\psi\rangle$: processo probabilistico che fa collassare $|\psi\rangle$ in $|\gamma\rangle_k$ con probabilità $|\langle\psi|\gamma\rangle_k|^2$

È una distribuzione di probabilità sui λ_k : $\sum_k |\langle\psi|\gamma\rangle_k|^2 = 1$

Valore atteso di A su $|\psi\rangle$: $\langle\psi|A|\psi\rangle$

Meccanica quantistica

Postulato 4: in un sistema fisico chiuso non si può distruggere informazione (Principio di Landauer + conservazione dell'energia).

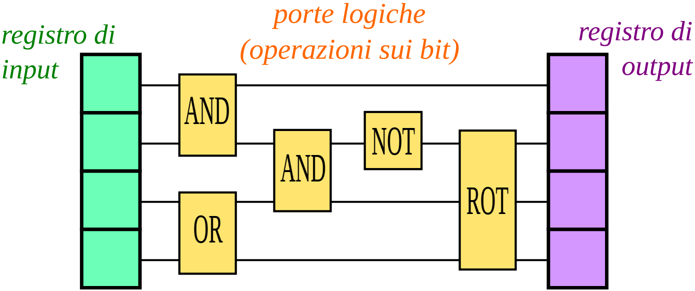
Quindi: trasformazione reversibile di un sistema $\leftrightsquigarrow$ operatore invertibile che mantiene norma e prodotto scalare (operatore unitario U, cioè $UU^\dagger = I$).

Esempio: operazione su n qubit $\leftrightsquigarrow$ matrice unitaria $2^n \times 2^n$.

Teorema: per ogni operatore unitario U esiste un unico operatore Hermitiano H tale che $U = e^{iH}$.

Circuiti classici

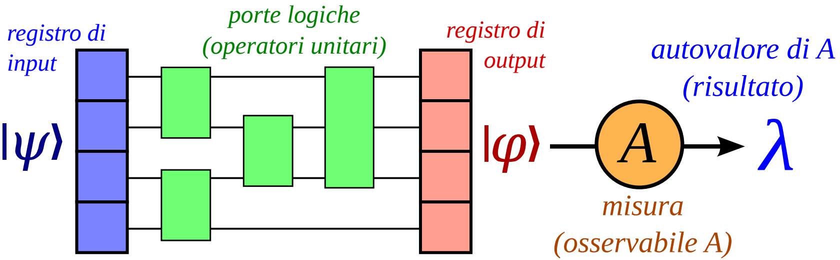
Circuito classico: modello astratto di calcolo equivalente a una macchina di Turing classica.



Circuiti quantistici

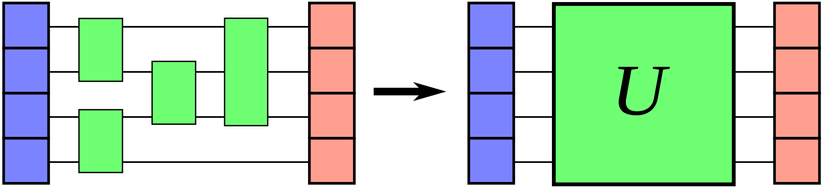
- il registro è un sistema fisico composto da n qubit invece che bit
- le porte logiche sono operatori unitari
- alla fine del calcolo, il risultato viene estratto dal registro di output tramite la misura di un osservabile A

Quindi questo modello è probabilistico.

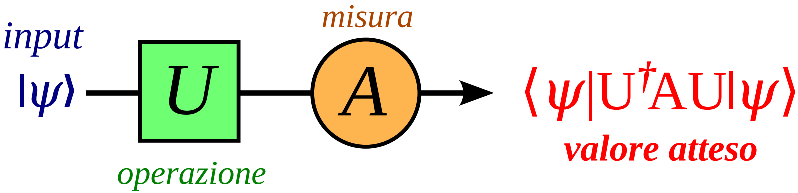


Circuiti quantistici

Tramite contrazione tensoriale: circuito $\leftrightsquigarrow$ operatore unitario U



Valore atteso della computazione a partire dall'input $|\psi\rangle$:



Simulabilità classica

Per n qubit: matrici $2^n \times 2^n \Longrightarrow$ calcolare $\langle\psi|U^\dagger A U|\psi\rangle$ classicamente in maniera diretta è generalmente difficile

Simulabilità classica: un circuito quantistico U su n qubit si dice (fortemente) efficientemente classicamente simulabile rispetto a:

- una classe di stati di input Ψ
- una classe di osservabili Ξ

se per ogni $|\psi\rangle \in \Psi$ e per ogni $A \in \Xi$ si può calcolare tramite un computer classico (macchina di Turing deterministica) il valore atteso $\langle\psi|U^\dagger A U|\psi\rangle$ fino a m cifre di precisione in tempo $\mathcal{O}(poly(n, m))$.

È una caratterizzazione molto forte. In generale si può fare solo per classi molto particolari di circuiti, stati e osservabili.

Matchgates

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, A, B \in U(2), \text{ con } det(A) = det(B).$$

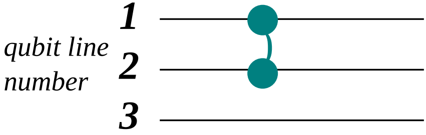
Matchgate: operatore su 2 qubit, che applica separatamente A e B sui due sottospazi bidimensionali di parità:

- spazio pari: generato da $|00\rangle$ e $|11\rangle$
- spazio dispari: generato da $|01\rangle$ e $|10\rangle$

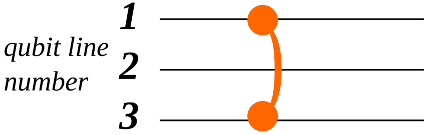
$$G(A, B) = \begin{pmatrix} a & 0 & 0 & b \\ 0 & e & f & 0 \\ 0 & g & h & 0 \\ c & 0 & 0 & d \end{pmatrix}$$

Matchgates

Nearest-neighbour (n.n.) matchgate: agisce su due qubit adiacenti:



Next-nearest-neighbour (n.n.n.) matchgate: agisce su due qubit distanti tra di loro solo un terzo qubit:



Teorema: n.n. e n.n.n. matchgates sono universali per il calcolo quantistico

Algebre di Clifford

Per un sistema di n qubit: $2n$ generatori $c_1, \ldots, c_{2n} : \mathcal{H} \to \mathcal{H}$

- $c_j = c_j^\dagger$, per ogni $j = 1, \ldots, 2n$
- $c_j c_k + c_k c_j = 2\delta_{j,k} I$, per ogni $j, k = 1, \ldots, 2n$
- $c_j^2 = (c_j^\dagger)^2 = I$, per ogni $j = 1, \ldots, 2n$

Algebra di Clifford (complessa): anello (formale) dei polinomi $\mathbb{C}[c_1, \ldots, c_{2n}]$ (grado formale massimo $2n$)

Rappresentazione di Jordan-Wigner:

$$c_{2k-1} = (Z_1 \otimes \ldots \otimes Z_{k-1} \otimes X_k \otimes I_{k+1} \otimes \ldots \otimes I_n)$$

$$c_{2k} = (Z_1 \otimes \ldots \otimes Z_{k-1} \otimes Y_k \otimes I_{k+1} \otimes \ldots \otimes I_n)$$

Operatori Gaussiani

Hamiltoniana Fermionica quadratica: combinazione lineare di termini quadratici nell'algebra di Clifford

$$H = \sum_{j,k=1}^{2n} \alpha_{j,k} c_j c_k$$

Operatore Gaussiano: operatore unitario generato da un'Hamiltoniana Fermionica quadratica:

$$U = e^{iH}$$

Teorema: gli operatori Gaussiani rappresentano circuiti quantistici fortemente efficientemente simulabili in modo classico, per una vastissima classe di stati e di osservabili

Simulabilità - N.n. matchgates

Notare i prodotti quadratici di generatori relativi a linee adiacenti:

$$\begin{array}{lll}
\mathbf{1} \;\text{———}\; & c_1\ c_2 & \\
\mathbf{2} \;\text{———}\; & c_3\ c_4 & \longrightarrow c_4 = (Z\ Y\ I) \\
\mathbf{3} \;\text{———}\; & c_5\ c_6 & \longrightarrow c_5 = (Z\ Z\ X)
\end{array}$$

$$\Downarrow$$

$$c_4 c_5 = i\,(I\ X\ X)$$

Questi prodotti agiscono solo sulle linee interessate.

Base per lo spazio delle matrici Hermitiane (X, Y, Z, I), separatamente nei due spazi di parità $\Longrightarrow$ n.n. matchgate generato tramite Hamiltoniana quadratica $\Longrightarrow$ operatore Gaussiano $\Longrightarrow$ simulabile efficientemente in maniera classica.

Simulabilità - N.n.n. matchgates

Per prodotti quadratici di generatori relativi a linee distanti invece:

$$
\begin{array}{lll}
\mathbf{1} \;\text{———}\; c_1 \; c_2 & \longrightarrow & c_2 = (Y\,I\,I) \\
\mathbf{2} \;\text{———}\; c_3 \; c_4 & & \\
\mathbf{3} \;\text{———}\; c_5 \; c_6 & \longrightarrow & c_5 = (Z\,Z\,X) \\
 & & \downarrow \\
 & & c_2\,c_5 = i\,(X\,Z\,X)
\end{array}
$$

Appare un'operatore stringa sulle linee intermedie.

N.n.n. matchgate agirebbe solo su linee 1 e 3 $\Longrightarrow$ non si può generalmente rappresentare come generato da un'Hamiltoniana di prodotti quadratici $\Longrightarrow$ no Gaussiano $\Longrightarrow$ non simulabile.

Riepilogo del risultato

Universalità di n.n. e n.n.n. matchgates

N.n. matchgates: classicamente simulabili

N.n.n. matchgates: non classicamente simulabili in genere

Enorme differenza computazionale dipendente solo da una proprietà topologica del circuito, insignificante nel caso di un circuito classico.

Tutta la potenza computazionale del computer quantistico sembra dipendere da questa proprietà topologica.

Nuovi risultati: eliminare l'operatore stringa

- usare $2n$ qubit: n qubit per sottosistema primario $+$ n qubit per sottosistema ausiliario
- rappresentare gli operatori in una sottoalgebra
- usare il sistema ausiliario come 'discarica' per eliminare gli operatori stringa
- separare l'operatore Gaussiano corrispondente come prodotto tensore di due operatori distinti
- simulare classicamente almeno il sottosistema primario

Nuova rappresentazione:

$$c_{2k-1} = (I_1 \dots I_{k-1} X_k I_{k+1} \dots I_n) \otimes (Z_{n+1} \dots Z_{n+k-1} X_{n+k} I_{n+k+1} \dots I_{2n})$$

$$c_{2k} = (I_1 \dots I_{k-1} Y_k I_{k+1} \dots I_n) \otimes (Z_{n+1} \dots Z_{n+k-1} X_{n+k} I_{n+k+1} \dots I_{2n})$$

Nuovi risultati: eliminare l'operatore stringa

Con questa nuova rappresentazione, per linee distanti:

$$\begin{array}{llll} \mathbf{1} & \text{———} & c_1\ c_2 & \longrightarrow c_2 = (Y\ I\ \ I) \otimes (X\ I\ \ I) \\ \mathbf{2} & \text{———} & c_3\ c_4 & \\ \mathbf{3} & \text{———} & c_5\ c_6 & \longrightarrow c_5 = (I\ \ I\ X) \otimes (Z\ Z\ X) \end{array}$$

$$c_2 c_5 = -i\,(Y\ I\ X) \otimes (Y\ Z\ X)$$

L'operatore stringa appare solo nel sistema ausiliario!

$$H = \sum_r \left(T_r^{prim} \oplus T_r^{aux} \right) \Longrightarrow U = e^{iH} = M \otimes V$$

Nuovi risultati: criterio sufficiente per la simulabilità dei n.n.n. matchgates

$n = 3 \Longrightarrow$ 6 generatori $c_1, \ldots, c_6 \Longrightarrow \frac{6\times(6-1)}{2} + 1 = 16$ prodotti quadratici indipendenti: $q_1, \ldots, q_{16}$

Prodotto interno matriciale: $((.,.)) \Longrightarrow$ ortonormalizzazione di Graham-Schmidt $\Longrightarrow$ elementi ortonormali $g_1, \ldots, g_{16}$

Criterio: un n.n.n. matchgate $M = e^{iH}$ è Gaussiano se e solo se vale la decomposizione:

$$H = \sum_{j=1}^{16} g_j((H, g_j))$$

nota: Gaussiano $\Rightarrow$ simulabile, ma non è detto il viceversa

Nuovi risultati: algoritmo per la ricerca di n.n.n. simulabili

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, B = \begin{pmatrix} e & f \\ g & h \end{pmatrix}, A, B \in U(2), \text{ con } det(A) = det(B).$$

struttura di H tale che $M = e^{iH}$ sia n.n.n. matchgate:

$$H = \begin{pmatrix} a & 0 & 0 & 0 & 0 & b & 0 & 0 \\ 0 & e & 0 & 0 & f & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & b \\ 0 & 0 & 0 & e & 0 & 0 & f & 0 \\ 0 & g & 0 & 0 & h & 0 & 0 & 0 \\ c & 0 & 0 & 0 & 0 & d & 0 & 0 \\ 0 & 0 & 0 & g & 0 & 0 & h & 0 \\ 0 & 0 & c & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

Nuovi risultati: algoritmo per la ricerca di n.n.n. simulabili

Algoritmo

- input: un set di scalari $\{ 0, \lambda_1, \ldots, \lambda_r \}$
- genera i termini quadratici $q_1, \ldots, q_{16}$
- testa tutte le combinazioni di $q_1, \ldots, q_{16}$ coi coefficienti dati
- se una combinazione ha la struttura di cui sopra, fermati e restituiscila
- se esaurisci tutte le possibili combinazioni restituisci errore (l'insieme di scalari in input non è adatto a generare un n.n.n. matchgate Gaussiano)

Conclusioni e sviluppi futuri

- poca ricerca sui n.n.n. matchgates finora, n.n. insoddisfacenti
- abbiamo dimostrato che n.n.n. matchgates Gaussiani esistono, sappiamo costruirli e sappiamo identificarli ove già dati
- possibilità di simulare classicamente l'algoritmo di Shor?
- nuovo framework per la rappresentazione di matchgate su linee arbitrarie, raddoppiare la 'memoria quantistica' (qubit) del sistema
- ricerca di Hamiltoniane di forma particolare, e loro classificazione
- possibilità di simulare classicamente nuove classi di circuiti quantistici?

Fine

Ringraziamenti

Dott. Marco Baioletti
Dott. Ivan Gerace
Dott. Simone Severini
Prof. Jens Eisert

Grazie a tutti per l'attenzione.