

Titolo della tesi:

Studio di simulatori e algoritmi quantistici.

Referente: Prof. M. Rosa Clot (rosaclot@tin.it, Tel. 055-4572297)

Con quantum computing si intende un nuovo modo di processare l'informazione basato su proprietà specifiche della meccanica quantistica. Benché la costruzione di un reale computer quantistico sia ancora lontana, le idee derivanti da questo nuovo tipo di programmazione stanno contribuendo allo sviluppo di nuove metodologie di calcolo, con applicazioni, per esempio, a importanti problemi di bioinformatica (il termine bioinformatica indica lo sviluppo e l'applicazione di metodi computazionali per l'analisi, l'interpretazione, la gestione e la predizione di dati genomici).

Il quantum computing sfrutta alcune caratteristiche fondamentali della meccanica quantistica: il principio di sovrapposizione degli stati, la linearità degli operatori di evoluzione, e gli effetti di interferenza, per ottenere dei vantaggi computazionali. L'unità elementare di informazione nel quantum computing non è infatti il bit, ma il qubit (quantum bit) che rappresenta lo stato quantistico di un sistema a due stati (per esempio lo spin di un elettrone, oppure il livello energetico di un sistema a due livelli). Il qubit, quindi, non è un numero binario, ma è rappresentabile matematicamente mediante un vettore in uno spazio di Hilbert bi-dimensionale (spazio vettoriale con coefficienti complessi e dotato di prodotto scalare). Al contrario del bit classico, che può assumere soltanto uno alla volta di due possibili valori, il qubit può essere in una qualsiasi sovrapposizione lineare di due stati fondamentali (stati di base). Questo implica che mentre un registro con L bits può assumere uno soltanto di 2^L valori, un registro di L qubits può contenere una sovrapposizione di stati con 2^L coefficienti complessi indipendenti e quindi codificare l'informazione relativa a 2^L stati contemporaneamente (per esempio, se $L=1000$ segue che $2^L = 2^{1000} > 10^{300}$). Calcolare una funzione di un certo registro quantistico di L qubits significa farlo evolvere mediante un certo operatore unitario su uno spazio di Hilbert L-dimensionale. La linearità di questo operatore permette di calcolare la funzione su tutti i 2^L stati di base contemporaneamente (parallelismo quantistico). In questo enorme parallelismo sta tutta la potenza del quantum computing. Questo non implica però un'equivalente potenza computazionale, poiché il processo di lettura di un registro quantistico corrisponde al processo di misura in meccanica quantistica, che proietta la sovrapposizione degli stati in uno qualsiasi di essi con una data probabilità. Parte del guadagno derivante dal parallelismo quantistico è comunque conservato, almeno in certi tipi di algoritmi, con notevoli vantaggi rispetto ai corrispondenti algoritmi classici.

In definitiva, un algoritmo quantistico è una sequenza di operazioni che trasforma lo stato iniziale del registro quantistico in modo tale che il processo finale di lettura dia il risultato corretto. Gli algoritmi quantistici più interessanti dal punto di vista applicativo sono, fino a questo momento, due: il metodo di Shor per la fattorizzazione di numeri interi e quello di Grover per la ricerca in un database non ordinato. Il primo algoritmo prevede un guadagno esponenziale (in termini di passi necessari) rispetto all'analogo classico, il secondo un guadagno quadratico (che è comunque significativo).

La tesi prevede lo studio della teoria dell'informazione quantistica, un'analisi comparativa dei simulatori esistenti per il quantum computing e la costruzione di un simulatore di pochi qubits (10-20) in Matlab, per lo sviluppo ed il test di algoritmi quantistici. La tesi prevede inoltre l'implementazione ed il test di alcuni algoritmi quantistici e il confronto con gli analoghi classici.