Corso di Formazione
Informatica Teorica e Quantum Computing
Prof. Marco Pedicini

IL CORSO DI **INFORMATICA TEORICA E QUANTUM COMPUTING** HA COME OBIETTIVO L'INTRODUZIONE DEI CONCETTI DI BASE PER LA SCIENZA DEI CALCOLATORI COME LA CALCOLABILITA', LA DECIDIBILITA' e LA COMPLESSITA' COMPUTAZIONALI E COME ORIZZONTE APPLICATIVO L'UTILIZZO NELLA DEFINIZIONE, NELLA PROGETTAZIONE E NELLO STUDIO DELLE CAPACITA' DEI CALCOLATORI BASATI SULLA MECCANICA QUANTISTICA.

Fisica e Computazione

Un processo di calcolo è essenzialmente un processo fisico che viene eseguito su una macchina il cui funzionamento obbedisce a determinate leggi fisiche. La teoria classica della computazione si basa su un modello astratto di macchina universale (la macchina di Turing) che funziona secondo un insieme di regole e di principi enunciati nel 1936 da Alan Turing e che elaborati successivamente da John von Neumann hanno portato negli anni '40 alla costruzione dei primi calcolatori.

Questi principi sono rimasti essenzialmente immutati da allora, nonostante gli enormi progressi tecnologici che permettono oggi di produrre dispositivi di gran lunga più potenti rispetto a quelli che si potevano realizzare nella prima metà del ventesimo secolo. La tacita assunzione alla base di questi principi è che una macchina di Turing idealizza un dispositivo meccanico di computazione (con una memoria potenzialmente infinita) che obbedisce alle leggi della fisica classica.

La computazione quantistica nasce come un paradigma alternativo basato sui principi della meccanica quantistica. Questi sono gli unici in grado di giustificare i fenomeni fisici che avvengono a livello microscopico, come per esempio all'interno di un atomo. Questi fenomeni saranno imprescindibili nella costruzione di computer elettronici in un futuro ormai prossimo se la legge di Moore continuerà a valere, come ci si aspetta. Questa legge formulata già negli anni Sessanta prevede che la potenza dei computer raddoppi una volta ogni due anni, per effetto della miniaturizzazione dei circuiti e la conseguente possibilità di farli lavorare a frequenze sempre maggiori. Questa legge ha dimostrato fino ad oggi la sua validità nella pratica, e gli effetti quantistici iniziano ad interferire nel funzionamento dei dispositivi elettronici man mano che le loro dimensioni diventano più piccole.

L'idea di realizzare un modello di computazione come un sistema quantistico isolato cominciò ad affacciarsi agli inizi degli anni ottanta, quando P. Benioff, partendo da considerazioni precedentemente elaborate da R. Landauer e C. Bennett, definì la Macchina di Turing reversibile: una computazione può sempre essere eseguita in modo da ritornare allo stato iniziale ripercorrendo all'indietro i vari passi di computazione. Successivamente R. Feynman dimostrò che nessuna Macchina di Turing classica poteva simulare certi fenomeni fisici senza incorrere in un rallentamento esponenziale delle sue prestazioni. Al contrario, un "simulatore quantistico universale" avrebbe potuto effettuare la simulazione in maniera più efficiente. Nel 1985, D. Deutsch formalizzò queste idee nella sua Macchina di Turing Quantistica Universale, che rappresenta in teoria della calcolabità quantistica esattamente quello che la Macchina di Turing Universale rappresenta per la calcolabità classica e ha portato alla concezione moderna di computazione quantistica. Naturalmente gli

effetti dell'introduzione del nuovo modello di calcolo si sono fatti sentire anche nel campo della complessità computazionale, (come previsto da Feynman), provocando il cambiamento della nozione di "trattabilità". Infatti, nel 1994 P. Shor dimostra che il problema della fattorizzazione dei numeri interi (classicamente considerato intrattabile) si può risolvere efficientemente (ovvero in tempo polinomiale) con un algoritmo quantistico. Questo risultato ha dato una forte spinta a tutto il settore poiché l'ipotesi di intrattabilità del problema della fattorizzazione di interi è alla base della sicurezza di alcuni algoritmi crittografici di largo impiego (RSA), quindi dimostrarne la trattabilità mette a rischio la sicurezza di molti (forse tutti) sistemi informatici. Queste considerazioni unite a quelle di tipo tecnologico accennate precedentemente, hanno portato all'affermarsi di un campo di ricerca oggi noto come teoria dell'informazione e della computazione quantistica. Concentrandoci su quest'ultima, ne studieremo le differenze fondamentali con il paradigma classico.

Queste derivano essenzialmente dai principi della teoria quantistica che regolano il mondo dell'infinitamente piccolo. In particolare, avremo a che fare con i tre fenomeni, tanto fondamentali quanto poco intuitivi, della teoria quantistica su cui la computazione quantistica si basa e che ne determinano l'enorme potenzialià di calcolo: il principio di sovrapposizione degli stati, il principio di misurazione e il fenomeno dell'entanglement.

Programma di massima

- Introduzione al concetto di computazione: macchine di Turing, problemi decidibili, macchine non-deterministiche, macchine probabilistiche, classi di complessità;
- Introduzione ai principi fondamentali della meccanica quantistica utilizzando il concetto di qubit (quantum bit) e di porta logica quantistica;
- Algoritmi quantistici di base come la trasformata di Fourier quantistica e l'algoritmo di fattorizzazione di Shor; le attese per algoritmi quantistici che risolvano problemi NP-completi;
- Le idee alla base della realizzazione pratica di computer quantistici.