Informazione e Calcolo Quantistico

(a partire dall'A.A. 2023/2024)

Proponenti: Proff. Gabriele Gianini, Carlo Mereghetti, Beatrice Palano
CdL: Triennale in Informatica
Cfu: 6 cfu per 48 ore di lezione frontale

Obiettivi Formativi

L'insegnamento presenta le basi del paradigma quantistico e della sua applicazione agli ambiti di comunicazione, crittografia e calcolo. Lo studente scoprirà alcune delle potenzialità delle tecnologie quantistiche attraverso esempi e successivamente consoliderà quanto ottenuto in un framework matematico che consente la modellizzazione dei sistemi quantistici negli ambiti sopra menzionati.

Risultati Apprendimento Attesi

Lo studente sarà in grado di comprendere i presupposti del paradigma quantistico e le motivazioni per la sua applicazione in diversi ambiti dell'informatica. Acquisirà la capacità di risolvere problemi elementari di meccanica quantistica di interesse ingegneristico (comunicazione e computazione quantistica). Apprenderà i principi di funzionamento di alcuni algoritmi paradigmatici per la distribuzione quantistica delle chiavi e di alcuni algoritmi di maggiore rilievo per il calcolo quantistico.

Programma (traccia)

Informazione quantistica e crittografia

- Particolarità dell'informazione quantistica e opportunità per comunicazione e crittografia.
- Indeterminazione delle misure quantistiche e generatori quantistici di numeri casuali.
- Sovrapposizione quantistica di stati e sfera di Bloch: dal Bit al Qbit. Notazione di Dirac.
- Variabili incompatibili e protocollo Bennett & Brassard 84 per la distribuzione di chiavi.
- Sistemi quantistici compositi: separabilità, entanglement e non-località quantistica.
- Protocollo Ekert 91 per la generazione di chiavi. Teletrasporto quantistico.
- Auto-interferenza; interaction-free measurement: Elitzur-Vaidman bomb tester.

Quantum Computing

- Un modello semplificato di computer: l'automa a stati finiti.
- Applicazione di diversi paradigmi di calcolo agli automi: determinismo, probabilismo e quantum.
- Punti di forza e di debolezza dei tre paradigmi nel mondo degli automi.
- Implementazione fisica di automi a stati finiti quantistici.
- Modelli di calcolo quantistico più generali.
- Il formalismo dei quantum gate array.
- I principali algoritmi quantistici: l'algoritmo di fattorizzazione di Shor, l'algoritmo di ricerca di Grover, il problema di Deutsch-Josza.

Testi

- Lucidi e dispense dell'insegnamento.
- M.A. Nielsen, I.L. Chuang. Quantum Computation and Quantum Information. Cambridge University Press, 2010.
- E. Rieffel, W.Polak. Quantum Computing – A Gentle Introduction. The MIT Press, 2011.