00-introduzione-corso-02

Quantum Computing

Introduzione

1

1

obiettivi formativi

- introduzione al modello di calcolo del quantum computing, con un approccio informatico

2

2

modelli di calcolo e informatica

- macchina di Turing
- lambda calcolo
- modelli per il calcolo parallelo e distribuito
- modelli per gerarchie di memorie
- molti altri modelli

3

3

programma

- quantum computing
  - qubit
  - coppie di qubit
  - registri
  - porte con uno o piu' qubit
  - no cloning theorem
  - l'operatore di Hadamard
  - computazioni reversibili
  - l'algoritmo di Bernstein Vazirani
  - l'algoritmo di Shor
  - teoria della complessità e quantum computing

4

4

testi consigliati (consultazione)

- *E. G. Rieffel, W. H. Polak*
  Quantum Computing: a Gentle Introduction
  MIT Press
- *N. S. Yanofsky, M. A. Mannucci*
  Quantum Computing for Computer Scientists
  Cambridge
- lezioni su Youtube di Umesh Vazirani (notevoli!)

5

5

quantum computing

- un nuovo modello di calcolo che
  - *potrebbe* essere fisicamente realizzabile
  - *potrebbe* avere un vantaggio esponenziale, in alcuni casi, rispetto ai computer tradizionali
- il modello pone una seria sfida alla *strong Church-Turing Thesis*
  - che dice che qualunque modello di calcolo può essere simulato da una Macchina di Turing con al più uno svantaggio polinomiale in termini di tempo

6

6

quantum e non-quantum

- anche se il quantum computing dovesse affermarsi è ipotizzabile che i computer tradizionali continuino ad essere usati per risolvere la maggior parte dei problemi

7

7

un po' di fisica

- per capire le basi del quantum computing occorre un pizzico di fisica
  - i parametri fisici (energia, momento, spin, ….) di una particella elementare (es. elettrone) sono quantizzati e possono assumere valori solo in un insieme discreto
  - gli stessi parametri ad un certo istante non hanno un valore che è un singolo numero; un parametro è invece associato a un'onda di probabilità (*superposition*)
  - un parametro assume un singolo valore (collassa a un singolo numero) quando viene osservato

8

8

qubit

- i computer tradizionali usano i bit, i cui valori possono essere 0 o 1
- i quantum computer usano i qubit
  - normalmente particelle subatomiche come elettroni o fotoni, in superposition
- generare e manipolare qubit è difficile
  - IBM, Google, Rigetti Computing usano circuiti superconduttori raffreddati a temperature più fredde dello spazio profondo
  - IonQ imprigiona atomi in campi elettromagnetici in camere ultra-high vacuum

9

9

due principali direzioni di lavoro

- sperimentale
  - costruzione di computer che sfruttano i fenomeni della meccanica quantistica
- teorica
  - quantum algorithms
    - progetto di algoritmi che sfruttano il modello di calcolo della meccanica quantistica
  - quantum protocols
    - progetto di protocolli per trasmettere e ricevere informazioni sfruttando il modello di calcolo della meccanica quantistica

10

10

assiomi

studiamo un modello di calcolo che consente di astrarre rispetto alla meccanica quantistica, basato su tre assiomi

1. superposition
2. misura
3. evoluzione unitaria

11

11

ostacoli

- vettori, matrici e un po' di algebra
- numeri complessi
- un po' di trigonometria
- pochissimo calcolo delle probabilità

12

12