Università di Genova

Macchine di Turing Quantistiche

Relatori

Elena Zucca

Francesco Dagnino

Candidato

Pietro Zignaigo

16-12-2024

Computazione quantistica

- **Quantum advantage**: A parità di problema, la complessità temporale degli algoritmi quantistici può essere minore di quella degli algoritmi classici.
- Lo stato di un computer quantistico è una sovrapposizione di stati discreti.

Computazione quantistica

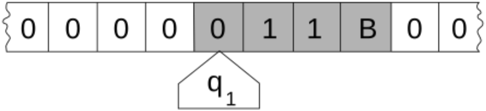
Spazi di Hilbert

- Per modellare uno stato quantistico si utilizzano gli *spazi di Hilbert*:

$$\ell^2(\mathcal{B}) = \left\{ \phi : \mathcal{B} \to \mathbb{C} \;\middle|\; \sum_{\mathcal{C} \in \mathcal{B}} |\phi(\mathcal{C})|^2 < \infty \right\}$$

- Per ragioni fisiche, possono essere applicati agli elementi dello spazio solo *operatori unitari*:
  - invertibili
  - conservano la norma

Macchina di Turing



- Modello matematico per una macchina che esegue un certo algoritmo.
- **Funzioni calcolabili**: Funzioni parziali $f : \mathbb{N} \to \mathbb{N}$ che sono calcolabili da una macchina di Turing.

Configurazioni

- Una configurazione, ovvero lo stato di una macchina di Turing, è una quadrupla:

$$\langle \alpha, q, \beta, i \rangle \in \Sigma^* \times \mathcal{Q} \times \Sigma^* \times \mathbb{Z}$$

- **Q-configurazioni**: Elementi di $\ell_1^2(\Sigma^* \times \mathcal{Q} \times \Sigma^* \times \mathbb{Z})$.

Configurazioni

Contatore

- Come mantenere inalterato il risultato dopo il raggiungimento di uno stato finale?
- Soluzione: aggiungere un contatore, la configurazione diventa:

$$\langle \alpha, q, \beta, i, n \rangle \in \Sigma^* \times \mathcal{Q} \times \Sigma^* \times \mathbb{Z} \times \mathbb{N}$$

  Chiamiamo questo insieme $\mathfrak{C}_M$.
- Le q-configurazioni diventano elementi di: $\ell_1^2 \left(\mathfrak{C}_M\right)$.

Funzione δ

Macchina di Turing Quantistica

■

Unitarietà

- Perché l'operatore, visto in forma matriciale, sia unitario:
  1. Deve avere le colonne con norma 1 (perché la norma sia sempre conservata)
  2. Ogni coppia di colonne deve essere ortogonale, ovvero due configurazioni pure non possono sovrapporsi dopo aver applicato l'operatore
- Esiste un teorema che garantisce l'unitarietà se δ rispetta certe condizioni.

Funzioni calcolabili quantistiche

- Una *Partial Probability Distribution (PPD)* è una funzione $\mathcal{P} : \mathbb{N} \to \mathbb{R}_{[0,1]}$ tale che $\sum_{n \in \mathbb{N}} \mathcal{P}(n) \leq 1$
- Una *Probability Distribution (PD)* è una *PPD* tale che $\sum_{n \in \mathbb{N}} \mathcal{P}(n) = 1$
- **Funzioni calcolabili quantistiche**: Funzioni $f : \ell_1^2(\mathbb{N}) \to PPD$ che sono calcolabili da una Macchina di Turing Quantistica.

Categorie di terminazione

Una data computazione può:

1. Produrre una *PD* in un numero di passi finito.
2. Non produrre una *PD* in un numero di passi finito, ma avere una *PD* come *PPD* limite.
3. Non avere una *PD* come *PPD* limite.

Misurazioni

-