Università di Genova

Macchine di Turing Quantistiche

Relatori

Elena Zucca

Francesco Dagnino

Candidato

Pietro Zignaigo

16-12-2024

Computazione quantistica

- Stato di un computer quantistico = sovrapposizione di stati discreti

Computazione quantistica

- Stato di un computer quantistico $=$ sovrapposizione di stati discreti
- L'unità minima di informazione quantistica è il *qubit*

$$1\,|\mathbf{0}\rangle + 0\,|\mathbf{1}\rangle$$

$$0\,|\mathbf{0}\rangle + 1\,|\mathbf{1}\rangle$$

$$\frac{1}{\sqrt{2}}\,|\mathbf{0}\rangle + \frac{1}{\sqrt{2}}\,|\mathbf{1}\rangle$$

$$\frac{1}{\sqrt{2}}\,|\mathbf{0}\rangle + i\frac{1}{\sqrt{2}}\,|\mathbf{1}\rangle$$

Computazione quantistica

- Osservazione ottiene 1 o 0, con probabilità dipendente dai pesi, distrugge parte dell'informazione, facendo collassare su $|0\rangle$ o su $|1\rangle$
- Quantum advantage: dato un problema, la complessità temporale degli algoritmi quantistici può essere minore di quella degli algoritmi classici

Modello matematico

Spazi di Hilbert

- Spazio di Hilbert generato da $\mathcal{B}$

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

- Prendiamo in considerazione solo ℓ_1^2

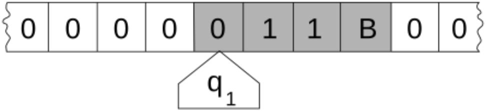
$$\ell_1^2(\mathcal{B}) = \left\{ \phi \in \ell^2(\mathcal{B}) \;\middle|\; \|\phi\|^2 = 1 \right\}$$

Modello matematico

Operatori

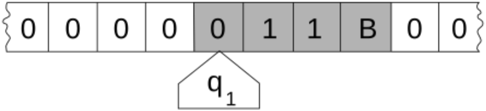
- TODO: trasformazione stato quantistico = operatore lineare = cioè una matrice B x B
- Possono essere usati solo operatori unitari
  - invertibili
  - conservano la norma
- In forma matriciale, sia unitario
  1. Deve avere colonne con norma 1 (perché la norma sia sempre conservata)
  2. Ogni coppia di colonne deve essere ortogonale

Macchina di Turing



- Modello matematico per descrivere tutti gli algoritmi
- Funzioni calcolabili: Funzioni parziali $f : \mathbb{N} \to \mathbb{N}$ modellabili da una macchina di Turing

Configurazioni



- Una configurazione di una macchina di Turing è

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

- Definiamo $\mathfrak{C}_M = \Sigma^* \times \mathcal{Q} \times \Sigma^* \times \mathbb{Z} \times \mathbb{N}$
- Q-configurazioni: elementi di $\ell_1^2(\mathfrak{C}_M) =$ sovrapposizione quantistica di configurazioni

Pre-macchina di Turing quantistica

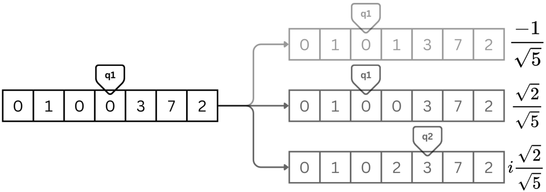
$$M = \langle \Sigma \times \mathcal{Q} \times \mathcal{Q}_s \times \mathcal{Q}_t \times \delta \times q_i \times q_f \rangle$$

- Funzione di transizione

$$\delta : (\mathcal{Q} \backslash \mathcal{Q}_t) \times \Sigma \rightarrow \ell_1^2 ((\mathcal{Q} \backslash \mathcal{Q}_s) \times \Sigma \times \mathbb{D})$$

Operatore di transizione

- Definiamo U_M su ogni $|C\rangle$ con $C \in \mathfrak{C}_M$



- Una pre-macchina di Turing quantistica è una macchina di Turing quantistica se U_M è unitario
  - Esiste un teorema che garantisce l'unitarietà se δ rispetta certe condizioni

Funzioni calcolabili quantistiche

PPD e computazioni

- 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 $\sum_{n \in \mathbb{N}} \mathcal{P}(n) = 1$
- A ogni $|\phi\rangle$ si può associare una PPD $\mathcal{P}_{|\phi\rangle}$
  $\mathcal{P}_{|\phi\rangle}(n) =$ probabilità di $|\phi\rangle$ di collassare su una configurazione finale con n simboli 1 sul nastro

Funzioni calcolabili quantistiche

PPD e computazioni

- Una computazione $K^M_{|\phi\rangle}$ è una sequenza $|\phi_i\rangle$ tale che
  1. $|\phi_0\rangle = |\phi\rangle$ è una q-configurazione finale
  2. $|\phi_i\rangle = U^i_M \, |\phi\rangle$
- A ogni computazione si associa una sequenza di PPD $\mathcal{P}_{|\phi_i\rangle}$
- La sequenza $\sum_{n \in \mathbb{N}} \mathcal{P}_{|\phi_i\rangle}(n)$ è crescente

Funzioni calcolabili quantistiche

Definizione

- Prendiamo in considerazione funzioni di forma $f : \ell_1^2(\mathbb{N}) \to PPD$
- $\mathcal{P} = \lim_{n\to\infty} \mathcal{P}_{|\phi_i\rangle}$ è l'output calcolato di M
- Scegliamo una codifica da $\ell_1^2(\mathbb{N})$ a $\ell_1^2\left(\mathfrak{C}_M^{init}\right)$
- Funzioni calcolabili quantistiche: Funzioni $f : \ell_1^2(\mathbb{N}) \to PPD$ rappresentabili 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

Conclusione

-