

UNIVERSITÀ DI GENOVA



**Università  
di Genova**

## Macchine di Turing Quantistiche

Relatori

*Elena Zucca*

*Francesco Dagnino*

Candidato

*Pietro Zignaigo*

16-12-2024

## Introduzione

- Computazione quantistica

- Modello matematico

- Macchina di Turing

## Macchina di Turing quantistica

- Configurazioni

- Macchina di Turing quantistica

- Operatore di transizione

## Funzioni calcolabili quantistiche

- PPD e computazioni

- Definizione

- Categorie di terminazione

## Conclusione

## Computazione quantistica

- Lo stato di un computer quantistico è una sovrapposizione di stati discreti
- L'unità minima di informazione quantistica è il *qubit*

$$[1, 0] = |0\rangle$$

$$\left[ \frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right] = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle$$

$$\left[ \frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right] = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle$$

- Osservazione distrugge parte dell'informazione, facendo collassare su  $|0\rangle$  o su  $|1\rangle$

# Computazione quantistica

---

Quantum advantage: A parità di problema, la complessità temporale degli algoritmi quantistici può essere minore di quella degli algoritmi classici

# Modello matematico

## Spazi di Hilbert

---

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

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

- Prendiamo in considerazione solo  $\ell_1^2$

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

# Modello matematico

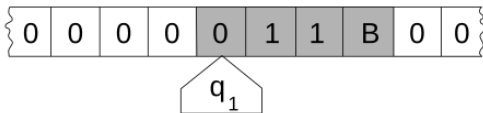
## Operatori

---

- L'equivalente delle porte logiche classiche sono gli operatori lineari
- Possono essere usati solo *operatori unitari*
  - invertibili
  - conservano la norma
- Perché l'operatore, visto 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, ovvero due configurazioni pure non possono sovrapporsi dopo aver applicato l'operatore

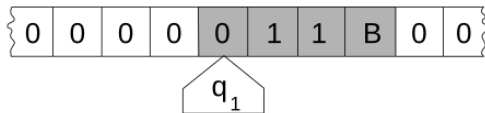
# Macchina di Turing

---



- Modello matematico per descrivere funzioni calcolabili da un algoritmo
- **Funzioni calcolabili:** Funzioni parziali  $f : \mathbb{N} \rightarrow \mathbb{N}$  modellabili da una macchina di Turing

# Configurazioni



- Una configurazione di una macchina di Turing è

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

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



# Macchina di Turing quantistica

---

- Una pre-macchina di Turing quantistica è una tupla

$$M = \langle \Sigma \times \mathcal{Q} \times \mathcal{Q}_s \times \mathcal{Q}_t \times \delta_0 \times q_i \times q_f \rangle$$

- Funzione  $\delta_0$

$$\delta_0 : (\mathcal{Q} \setminus \mathcal{Q}_t) \times \Sigma \rightarrow \ell_1^2((\mathcal{Q} \setminus \mathcal{Q}_s) \times \Sigma \times \mathbb{D})$$

- Una pre-macchina di Turing quantistica è una macchina di Turing quantistica se l'operatore di transizione  $U_M$  è unitario

# Operatore di transizione

---

- Definiamo  $U_M$  su ogni  $|C\rangle$  con  $C \in \mathfrak{C}_M$
- Se  $C \in \mathfrak{C}_M^0 \setminus \mathfrak{C}_M^t$

$$U_M(|C\rangle) = \sum_{(p,v,d) \in (\mathcal{Q} \setminus \mathcal{Q}_s) \times \Sigma \times \mathbb{D}} \delta_0(q, u)(p, v, d) |C_{p,v,d}\rangle$$

- Esiste un teorema che garantisce l'unitarietà se  $\delta_0$  rispetta certe condizioni

# Funzioni calcolabili quantistiche

## PPD e computazioni

---

- Una *Partial Probability Distribution (PPD)* è una funzione  $\mathcal{P} : \mathbb{N} \rightarrow \mathbb{R}_{[0,1]}$  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  $K_{|\phi\rangle}^M$  è una sequenza  $|\phi_i\rangle$  tale che
  1.  $|\phi_0\rangle = |\phi\rangle$  è una q-configurazione finale
  2.  $|\phi_i\rangle = U_M^i |\phi\rangle$
- 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  $f : \ell_1^2(\mathbb{N}) \rightarrow PPD$
- $\mathcal{P} = \lim_{n \rightarrow \infty} \mathcal{P}_{|\phi_i\rangle}$  è l'*output calcolato* di  $M$
- Scegliamo una codifica da  $\ell_1^2(\mathbb{N})$  a  $\ell_1^2(\mathfrak{C}_M^{init})$
- **Funzioni calcolabili quantistiche:** Funzioni  $f : \ell_1^2(\mathbb{N}) \rightarrow PPD$  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

---

