

UNIVERSITÀ DI GENOVA



**Università
di Genova**

Macchine di Turing Quantistiche

Relatori

Francesco Dagnino

Elena Zucca

Candidato

Pietro Zignaigo

16-12-2024

Introduzione

Macchina di Turing quantistica

Funzioni calcolabili quantistiche

Conclusione

Computazione quantistica

- Informazione in un computer quantistico = sovrapposizione di stati discreti

Computazione quantistica

- Informazione in un computer quantistico = sovrapposizione di stati discreti
- Unità minima di informazione quantistica: **qubit**

$$1|0\rangle + 0|1\rangle \quad 0|0\rangle + 1|1\rangle$$

Computazione quantistica

- Informazione in un computer quantistico = sovrapposizione di stati discreti
- Unità minima di informazione quantistica: **qubit**

$$1|0\rangle + 0|1\rangle \quad 0|0\rangle + 1|1\rangle$$

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

Computazione quantistica

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

■ Osservazione:

- Si ottiene 1 o 0
- Probabilità dipendente dai pesi
- Collasso su $|0\rangle$ o su $|1\rangle$

Computazione quantistica

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

- Osservazione:
 - Si ottiene 1 o 0
 - Probabilità dipendente dai pesi
 - Collasso su $|0\rangle$ o su $|1\rangle$
- Quantum advantage: per certi problemi, complessità algoritmi quantistici < complessità algoritmi classici

Modello matematico

Spazi di Hilbert

- Spazio di Hilbert generato da \mathcal{B}

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

Modello matematico

Spazi di Hilbert

- Spazio di Hilbert generato da \mathcal{B}

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

- Prendiamo in considerazione solo ℓ_1^2

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

Modello matematico

Operatori

- Trasformazione stato quantistico = operatore lineare = matrice $\mathcal{B} \times \mathcal{B}$

Modello matematico

Operatori

- Trasformazione stato quantistico = operatore lineare = matrice $\mathcal{B} \times \mathcal{B}$
- Possono essere usati solo operatori unitari
 - invertibili \rightarrow meccanica quantistica è reversibile
 - conservano la norma \rightarrow per rimanere in $\ell_1^2(\mathcal{B})$

Modello matematico

Operatori

- Trasformazione stato quantistico = operatore lineare = matrice $\mathcal{B} \times \mathcal{B}$
- Possono essere usati solo **operatori unitari**
 - invertibili \rightarrow meccanica quantistica è reversibile
 - conservano la norma \rightarrow per rimanere in $\ell_1^2(\mathcal{B})$
- Unitarietà in forma matriciale
 - Colonne con norma 1 (per conservare la norma)
 - Ogni coppia di colonne deve essere ortogonale

Macchina di Turing

fino ad ora

modello fisico (hardware)

- basato su qbit
- estende circuiti classici

Macchina di Turing

fino ad ora

modello fisico (hardware)

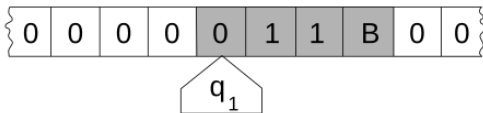
- basato su qbit
- estende circuiti classici

obiettivo

formalismo più astratto (software)

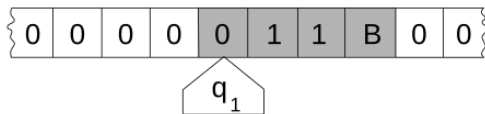
- descrive tutti gli algoritmi quantistici
- estende Macchine di Turing classiche

Macchina di Turing



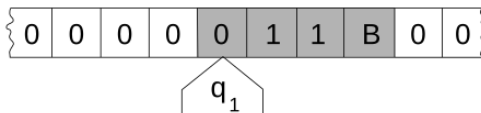
- Modello matematico per descrivere tutti gli algoritmi

Macchina di Turing



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

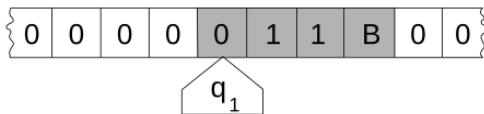
Configurazioni



Configurazione di una macchina di Turing

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

Configurazioni

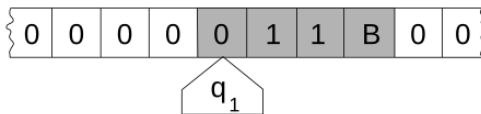


Configurazione di una macchina di Turing

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

$$\mathfrak{C}_M = \Sigma^* \times Q \times \Sigma^* \times \mathbb{Z} \times \mathbb{N}$$

Configurazioni



$$\mathfrak{C}_M = \Sigma^* \times \mathcal{Q} \times \Sigma^* \times \mathbb{Z} \times \mathbb{N}$$

Q-configurazione

elemento di $\ell_1^2(\mathfrak{C}_M)$ = sovrapposizione di configurazioni

Pre-macchina di Turing quantistica

$$M = \langle \Sigma \times Q \times Q_s \times Q_t \times \delta \times q_i \times q_f \rangle$$

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

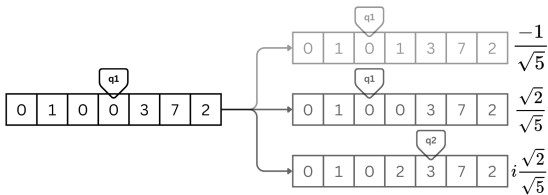
$$\delta : (\mathcal{Q} \setminus \mathcal{Q}_t) \times \Sigma \rightarrow \ell_1^2((\mathcal{Q} \setminus \mathcal{Q}_s) \times \Sigma \times \mathbb{D})$$

Operatore di transizione

- $U_M : \ell^2(\mathfrak{C}_M) \rightarrow \ell^2(\mathfrak{C}_M)$

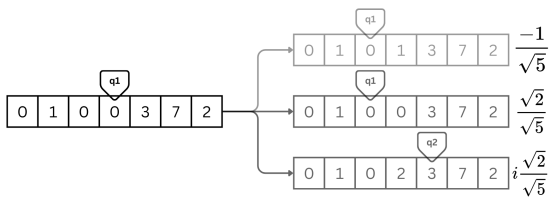
Operatore di transizione

- $U_M : \ell^2(\mathfrak{C}_M) \rightarrow \ell^2(\mathfrak{C}_M)$
- Definiamo U_M su ogni $C \in \mathfrak{C}_M$



Operatore di transizione

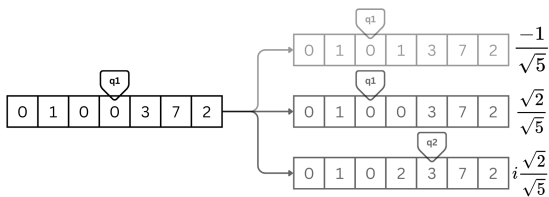
- $U_M : \ell^2(\mathfrak{C}_M) \rightarrow \ell^2(\mathfrak{C}_M)$
- Definiamo U_M su ogni $C \in \mathfrak{C}_M$



- Una pre-macchina di Turing quantistica è una **macchina di Turing quantistica** se U_M è unitario

Operatore di transizione

- $U_M : \ell^2(\mathfrak{C}_M) \rightarrow \ell^2(\mathfrak{C}_M)$
- Definiamo U_M su ogni $C \in \mathfrak{C}_M$



- Una pre-macchina di Turing quantistica è una **macchina di Turing quantistica** se U_M è unitario
- U_M unitario se δ rispetta certe condizioni

Computazioni e osservazioni

- Una **computazione** è una sequenza $(\phi_i)_{i \in \mathbb{N}}$ con ϕ_0 iniziale tale che

$$\phi_0 \rightarrow \phi_1 = U_M(\phi_0) \rightarrow \dots \rightarrow \phi_i = U_M(\phi_{i-1}) \rightarrow \dots$$

Computazioni e osservazioni

- Una **computazione** è una sequenza $(\phi_i)_{i \in \mathbb{N}}$ con ϕ_0 iniziale tale che

$$\phi_0 \rightarrow \phi_1 = U_M(\phi_0) \rightarrow \dots \rightarrow \phi_i = U_M(\phi_{i-1}) \rightarrow \dots$$

$$\mathcal{P}_{\phi_0} \rightarrow \mathcal{P}_{\phi_1} \longrightarrow \dots \rightarrow \mathcal{P}_{\phi_i} \longrightarrow \dots$$

$\mathcal{P}_\phi(n)$ = probabilità di ottenere una configurazione finale con n simboli 1 sul nastro osservando ϕ

Computazioni e osservazioni

- Una **computazione** è una sequenza $(\phi_i)_{i \in \mathbb{N}}$ con ϕ_0 iniziale tale che

$$\begin{array}{ccccccc} \phi_0 & \rightarrow & \phi_1 = U_M(\phi_0) & \rightarrow & \dots & \rightarrow & \phi_i = U_M(\phi_{i-1}) \rightarrow \dots \\ \mathcal{P}_{\phi_0} & \rightarrow & \mathcal{P}_{\phi_1} & \longrightarrow & \dots & \rightarrow & \mathcal{P}_{\phi_i} \longrightarrow \dots \end{array}$$

$\mathcal{P}_\phi(n)$ = probabilità di ottenere una configurazione finale con n simboli 1 sul nastro osservando ϕ

- **Partial Probability Distribution (PPD)**: funzione $\mathcal{P} : \mathbb{N} \rightarrow \mathbb{R}_{[0,1]}$ tale che $\sum_{n \in \mathbb{N}} \mathcal{P}(n) \leq 1$
Probability Distribution (PD): *PPD* tale che $\sum_{n \in \mathbb{N}} \mathcal{P}(n) = 1$

Funzioni calcolabili quantistiche

- Ci interessano funzioni di forma

$$f : \ell_1^2(\mathbb{N}) \rightarrow PPD$$

Funzioni calcolabili quantistiche

- Ci interessano funzioni di forma

$$f : \ell_1^2(\mathbb{N}) \rightarrow PPD$$

- Codifichiamo $\ell_1^2(\mathbb{N})$ in $\ell_1^2(\mathfrak{C}_M^{init})$

Funzioni calcolabili quantistiche

- Ci interessano funzioni di forma

$$f : \ell_1^2(\mathbb{N}) \rightarrow PPD$$

- Codifichiamo $\ell_1^2(\mathbb{N})$ in $\ell_1^2(\mathfrak{C}_M^{init})$
- $f_M(\psi) = \lim_{i \rightarrow \infty} \mathcal{P}_{\phi_i}$ è la **funzione calcolata** da M
 $\phi_0 = \text{codifica di } \psi \in \ell_1^2(\mathbb{N})$

Funzioni calcolabili quantistiche

- Ci interessano funzioni di forma

$$f : \ell_1^2(\mathbb{N}) \rightarrow PPD$$

- Codifichiamo $\ell_1^2(\mathbb{N})$ in $\ell_1^2(\mathfrak{C}_M^{init})$
- $f_M(\psi) = \lim_{i \rightarrow \infty} \mathcal{P}_{\phi_i}$ è la **funzione calcolata** da M
 $\phi_0 = \text{codifica di } \psi \in \ell_1^2(\mathbb{N})$
- **Funzioni calcolabili quantistiche**: funzioni della forma f_M

Categorie di terminazione

Una data computazione può

1. Produrre una PD in un numero di passi finito

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 limite (*Almost sure termination*)

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 limite (*Almost sure termination*)
3. Non avere una PD come PPD limite

Conclusione

- Il modello di MTQ qui presentato è quello di Guerrini, Martini e Masin, pubblicato nel 2020

Conclusione

- Il modello di MTQ qui presentato è quello di Guerrini, Martini e Masin, pubblicato nel 2020
- Non ho parlato del protocollo di misurazione

Conclusione

- Il modello di MTQ qui presentato è quello di Guerrini, Martini e Masin, pubblicato nel 2020
- Non ho parlato del protocollo di misurazione
- Esistono modelli precedenti, in particolare quello di Deutsch (1985) e di Bernstein e Vazirani (1997)

Grazie per l'attenzione!