Università di Genova

Macchine di Turing Quantistiche

Relatori

Elena Zucca

Francesco Dagnino

Candidato

Pietro Zignaigo

16-12-2024

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

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

Computazione quantistica

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

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

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

Computazione quantistica

- Osservazione:
  - Si ottiene 1 o 0
  - Probabilità dipendente dai pesi
  - Collasso su $|\mathbf{0}\rangle$ o su $|\mathbf{1}\rangle$

Computazione quantistica

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

Modello matematico

Spazi di Hilbert

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

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

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^2_1

$$\ell^2_1(\mathcal{B}) = \left\{ \phi \in \ell^2(\mathcal{B}) \;\middle|\; \|\phi\|^2 = 1 \right\}$$

Modello matematico

Operatori

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

Modello matematico

Operatori

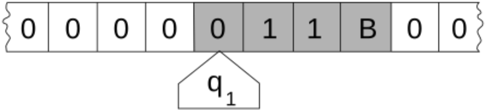
- Trasformazione stato quantistico = operatore lineare = matrice $\mathcal{B} \times \mathcal{B}$
- Possono essere usati solo operatori unitari
  - invertibili $\rightarrow$ meccanica quantistica è reversibile
  - conservano la norma $\rightarrow$ per rimanere in $\ell_1^2(\mathcal{B})$

Modello matematico

Operatori

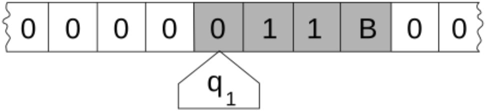
- Trasformazione stato quantistico = operatore lineare = matrice $\mathcal{B} \times \mathcal{B}$
- Possono essere usati solo operatori unitari
  - invertibili $\rightarrow$ meccanica quantistica è reversibile
  - conservano la norma $\rightarrow$ per rimanere in $\ell_1^2(\mathcal{B})$
- Unitarietà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

Macchina di Turing



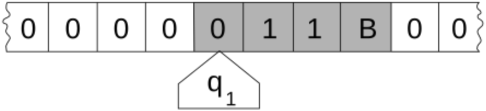
- Modello matematico per descrivere tutti gli algoritmi

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

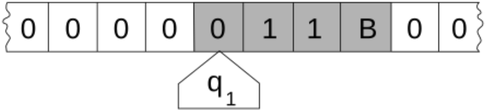
Configurazioni



Configurazione di una macchina di Turing

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

Configurazioni

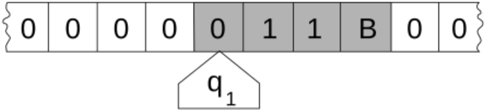


Configurazione di una macchina di Turing

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

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

Configurazioni



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

Q-configurazione

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

Pre-macchina di Turing quantistica

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

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

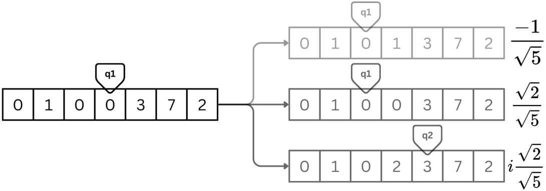
$$\delta : (\mathcal{Q} \backslash \mathcal{Q}_t) \times \Sigma \rightarrow \ell_1^2((\mathcal{Q} \backslash \mathcal{Q}_s) \times \Sigma \times \mathbb{D})$$

Operatore di transizione

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

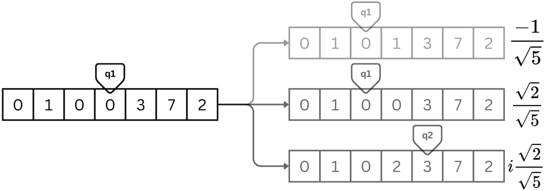
Operatore di transizione

- $U_M : \ell^2(\mathfrak{C}_M) \to \ell^2(\mathfrak{C}_M)$
- Definiamo U_M su ogni $|C\rangle$ con $C \in \mathfrak{C}_M$



Operatore di transizione

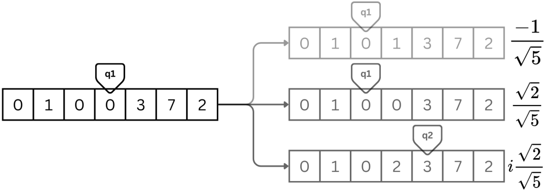
- $U_M : \ell^2(\mathfrak{C}_M) \to \ell^2(\mathfrak{C}_M)$
- Definiamo U_M su ogni $|C\rangle$ con $C \in \mathfrak{C}_M$



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

Operatore di transizione

- $U_M : \ell^2(\mathfrak{C}_M) \to \ell^2(\mathfrak{C}_M)$
- 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
- U_M unitario se δ rispetta certe condizioni

Funzioni calcolabili quantistiche

PPD e computazioni

- Una computazione è una sequenza $|\phi_i\rangle$ tale che

$$|\phi_i\rangle = U_M^i|\phi\rangle$$

$|\phi_0\rangle$ è una q-configurazione iniziale

Funzioni calcolabili quantistiche

PPD e computazioni

- Una computazione è una sequenza $|\phi_i\rangle$ tale che
$$|\phi_i\rangle = U_M^i|\phi\rangle$$
$|\phi_0\rangle$ è una q-configurazione iniziale
- 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

PPD e computazioni

- Una computazione è una sequenza $|\phi_i\rangle$ tale che
$$|\phi_i\rangle = U_M^i|\phi\rangle$$
$|\phi_0\rangle$ è una q-configurazione iniziale
- 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 ottenere una configurazione finale con n simboli 1 sul nastro osservando $|\phi\rangle$

Funzioni calcolabili quantistiche

PPD e computazioni

- Una computazione è una sequenza $|\phi_i\rangle$ tale che
$$|\phi_i\rangle = U_M^i |\phi\rangle$$
$|\phi_0\rangle$ è una q-configurazione iniziale
- 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 ottenere una configurazione finale con n simboli 1 sul nastro osservando $|\phi\rangle$
- A ogni computazione si associa una sequenza di PPD $\mathcal{P}_{|\phi_i\rangle}$

Funzioni calcolabili quantistiche

PPD e computazioni

- Una computazione è una sequenza $|\phi_i\rangle$ tale che
$$|\phi_i\rangle = U_M^i|\phi\rangle$$
$|\phi_0\rangle$ è una q-configurazione iniziale
- 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 ottenere una configurazione finale con n simboli 1 sul nastro osservando $|\phi\rangle$
- 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

- Ci interessano funzioni di forma $f : \ell_1^2(\mathbb{N}) \to PPD$

Funzioni calcolabili quantistiche

Definizione

- Ci interessano 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 $\ell_1^2(\mathfrak{C}_M^{init})$

Funzioni calcolabili quantistiche

Definizione

- Ci interessano 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 $\ell_1^2(\mathfrak{C}_M^{init})$
- Funzioni calcolabili quantistiche: Funzioni $f : \ell_1^2(\mathbb{N}) \to PPD$ modellabili da una Macchina di Turing quantistica

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 *PPD* limite

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