40-no-cloning-theorem-03.pdf

Quantum Computing

No cloning theorem

1

1

impossibilità di copiare un qubit

- un qubit non può essere copiato in un altro qubit!
- supponiamo di avere un qubit $|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ e di volerlo copiare in un qubit che inizialmente è in un altro stato, ad es. $|0\rangle$
- ovviamente non possiamo misurare $|\psi\rangle$
  - altrimenti perdiamo i valori α_0 e α_1
- dobbiamo quindi cavarcela costruendo un circuito apposito

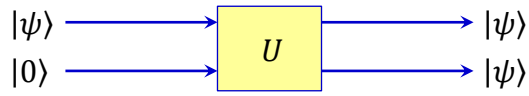
2

2

40-no-cloning-theorem-03.pdf

un circuito per copiare un qubit

- supponiamo, per assurdo, che esista un circuito U (unitary transformation) che ci consenta di fare la copia
- dovrà avere i seguenti input e output



3

3

una funzione per copiare un qubit

- il circuito dovrebbe implementare una funzione U tale che $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle \xrightarrow{U} (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle) \; \forall \alpha_0, \alpha_1 \in \mathbb{C}$
- oppure $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ 0 \\ \alpha_1 \\ 0 \end{pmatrix} \xrightarrow{U} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\alpha_0 \\ \alpha_0\alpha_1 \\ \alpha_1\alpha_0 \\ \alpha_1\alpha_1 \end{pmatrix}$
- in altri termini $\alpha_0|00\rangle + \alpha_1|10\rangle \xrightarrow{U} \alpha_0^2|00\rangle + \alpha_0 \alpha_1|10\rangle + \alpha_0\alpha_1|01\rangle + \alpha_1^2|11\rangle$

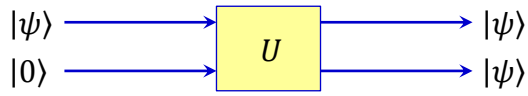
4

4

40-no-cloning-theorem-03.pdf

una funzione per copiare un qubit

- il circuito dovrebbe implementare una funzione U tale che $\alpha_0|00\rangle + \alpha_1|10\rangle \xrightarrow{U} \alpha_0^2|00\rangle + \alpha_0 \alpha_1|10\rangle + \alpha_0\alpha_1|01\rangle + \alpha_1^2|11\rangle \; \forall \alpha_0, \alpha_1 \in \mathbb{C}$
- se U esiste, allora deve funzionare anche per $\alpha_0 = 1$ e $\alpha_1 = 0$ e per $\alpha_0 = 0$ e $\alpha_1 = 1$
- quindi $|00\rangle \xrightarrow{U} |00\rangle$ e $|10\rangle \xrightarrow{U} |11\rangle$

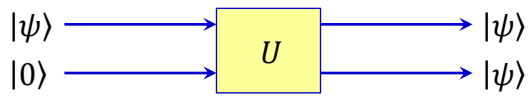


5

5

impossibilità della copia

- quindi se applichiamo U allo specifico stato $\alpha_0|00\rangle + \alpha_1|10\rangle$ otteniamo, per linearità, $\alpha_0|00\rangle + \alpha_1|10\rangle \xrightarrow{U} \alpha_0 U|00\rangle + \alpha_1 U|10\rangle = \alpha_0|00\rangle + \alpha_1|11\rangle$
- che è diverso da ciò che volevamo ottenere, cioè $\alpha_0|00\rangle + \alpha_1|10\rangle \xrightarrow{U} \alpha_0^2|00\rangle + \alpha_0\alpha_1|10\rangle + \alpha_0\alpha_1|01\rangle + \alpha_1^2|11\rangle$



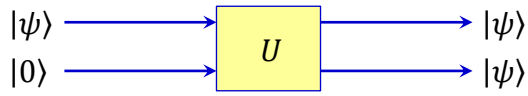
6

6

40-no-cloning-theorem-03.pdf

impossibilità della copia

- quindi U non esiste (!)
- attenzione: il fatto che la copia non sia possibile in generale non implica che non sia possibile costruire specifici stati noti a partire da altri specifici stati noti



7

7

esercizio – $SWAP$ gate

- è possibile almeno realizzare un circuito che scambi tra loro due qubit?
- se sì, mostrare la matrice dell'operatore

8

8

40-no-cloning-theorem-03.pdf

progettazione – $SWAP$ gate

- se esiste dovrà funzionare anche sugli stati di base, per cui
  - $|00\rangle \xrightarrow{SWAP} |00\rangle$
  - $|01\rangle \xrightarrow{SWAP} |10\rangle$
  - $|10\rangle \xrightarrow{SWAP} |01\rangle$
  - $|11\rangle \xrightarrow{SWAP} |11\rangle$

9

9

progettazione – $SWAP$ gate

- possiamo progettare la matrice a partire dagli stati base
  - $|00\rangle \xrightarrow{SWAP} |00\rangle$
  - $|01\rangle \xrightarrow{SWAP} |10\rangle$
  - $|10\rangle \xrightarrow{SWAP} |01\rangle$
  - $|11\rangle \xrightarrow{SWAP} |11\rangle$

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

10

10

40-no-cloning-theorem-03.pdf

unitary – $SWAP$ gate

- verifichiamo se è una unitary transformation:

$$SWAP = SWAP^{\dagger} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

11

11

qubit qualunque – $SWAP$ gate

- ricordiamo che $SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$
- con input $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} \otimes \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix}$ abbiamo $SWAP \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_0 \\ \alpha_1\beta_1 \end{pmatrix} = \begin{pmatrix} \alpha_0\beta_0 \\ \alpha_1\beta_0 \\ \alpha_0\beta_1 \\ \alpha_1\beta_1 \end{pmatrix} = \begin{pmatrix} \beta_0 \\ \beta_1 \end{pmatrix} \otimes \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = (\beta_0|0\rangle + \beta_1|1\rangle) \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle)$

12

12