Quantum Computing

Alessandra Di Pierro

1 Esercitazione 5: Misurare nei circuiti quantistici

Un'applicazione importante del Postulato 3 sulla misurazione quantistica riguarda il problema di *distinguere stati quantistici*. In meccanica quantistica, stati non ortogonali non possono essere distinti, cioé non esiste nessuna misurazione che permetta di stabilire con probabilitá 1 qual'é lo stato che stiamo misurando. Al contrario, se gli stati sono ortogonali é sempre possibile distinguerli. Infatti, é sufficiente eseguire una misurazione definita mediante gli operatori di proiezione $P_m = |m\rangle\langle m|$ (dove $\{|m\rangle\}$ formano un insieme ortonormale di stati), tali che $\sum_m P_m = I$. Si verifica facilmente che una misurazione nello stato $|m\rangle$ dá come risultato m con probabilitá $\langle m| P_m |m\rangle = 1$.

Una dimostrazione formale del fatto che non esiste nessuna misurazione in grado di distinguere due stati non ortogonali $|\psi_1\rangle$ e $|\psi_2\rangle$ si puó ottenere per contraddizione.
Supponiamo che tale misurazione esista. Allora esisteranno operatori E_1 e E_2 tali che

$$\langle\psi_1| E_1 |\psi_1\rangle = 1 \text{ e } \langle\psi_2| E_2 |\psi_2\rangle = 1.$$

Poiché $\sum_i E_i = I$, segue che $\sum_i \langle\psi_1| E_i |\psi_1\rangle = 1$ e quindi $\langle\psi_1| E_2 |\psi_1\rangle = 0$, cioé $\langle\psi_1| \sqrt{E_2}\sqrt{E_2} |\psi_1\rangle = 0$, da cui segue $\sqrt{E_2}|\psi_1\rangle = 0$. Dall'ipotesi di non ortogonalitá di $|\psi_1\rangle$ e $|\psi_2\rangle$, possiamo decomporre $|\psi_2\rangle$ in una componente parallela a $|\psi_1\rangle$ ed una, $|\varphi\rangle$, ortogonale a $|\psi_1\rangle$, cioé possiamo scrivere $|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$, con $|\alpha|^2 + |\beta|^2 = 1$ e $|\beta| < 1$. Otteniamo quindi che $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$. Ma allora

$$\langle\psi_2| E_2 |\psi_2\rangle = |\beta|^2 \langle\varphi| E_2 |\varphi\rangle,$$

che é in contraddizione con l'ipotesi che $\langle\psi_2| E_2 |\psi_2\rangle = 1$. Infatti, poiché

$$\langle\varphi| E_2 |\varphi\rangle \leq \sum_i \langle\varphi| E_i |\varphi\rangle = \langle\varphi|\varphi\rangle = 1,$$

si ha che $|\beta|^2 \langle\varphi| E_2 |\varphi\rangle \leq |\beta|^2 < 1$ e quindi $\langle\psi_2| E_2 |\psi_2\rangle < 1$.

Esercizio 1.1 (Distinguere stati quantistici) *Il sistema A viene preparato in uno dei due stati* non ortogonali $|\varphi\rangle$ *o* $|\tilde{\varphi}\rangle$*. Si vuole conoscere lo stato in cui si trova A senza disturbarlo. Per far questo si prepari un altro sistema B in uno stato $|\beta\rangle$ e si applichi al sistema composto AB una trasformazione unitaria U che trasforma lo stato composto nel seguente modo:*

$$\begin{aligned} |\Psi\rangle = |\varphi\rangle \otimes |\beta\rangle &\quad\to\quad \left|\Psi'\right\rangle = |\varphi\rangle \otimes \left|\beta'\right\rangle \\ \left|\tilde{\Psi}\right\rangle = |\tilde{\varphi}\rangle \otimes |\beta\rangle &\quad\to\quad \left|\tilde{\Psi}'\right\rangle = |\tilde{\varphi}\rangle \otimes \left|\tilde{\beta}'\right\rangle, \end{aligned}$$

lasciando effettivamente indisturbato lo stato del sistema A. Si esegua ora una misurazione sul sistema B che permetta di distinguere gli stati $|\beta'\rangle$ e $\left|\tilde{\beta}'\right\rangle$.

1. *É possibile trovare una tale trasformazione unitaria U, nell'ipotesi di non-ortogonalitá degli stati $|\varphi\rangle$ e $|\tilde{\varphi}\rangle$?*
2. *Cosa cambia se gli stati $|\varphi\rangle$ e $|\tilde{\varphi}\rangle$ sono ortogonali?*

Soluzione

1. Se esistesse una trasformazione unitaria U tale da trasformare il sistema ausiliario B in due stati $|\beta'\rangle$ o $\left|\tilde{\beta}'\right\rangle$ distinguibili con probabilitá 1, allora dovremmo concludere che é sempre possibile distinguere due stati non ortogonali come $|\varphi\rangle$ e $|\tilde{\varphi}\rangle$, contrariamente a quanto dimostrato precedentemente.

   Vediamo formalmente l'effetto che avrebbe U sugli stati di input $|\Psi\rangle$ e $\left|\tilde{\Psi}\right\rangle$. Notiamo che

   $$\begin{aligned} \left\langle \tilde{\Psi}' \middle| \Psi' \right\rangle &= \langle\tilde{\varphi}|\varphi\rangle \left\langle \tilde{\beta}' \middle| \beta' \right\rangle \\ \left\langle \tilde{\Psi} \middle| \Psi \right\rangle &= \langle\tilde{\varphi}|\varphi\rangle \left\langle \tilde{\beta} \middle| \beta \right\rangle = \langle\tilde{\varphi}|\varphi\rangle \end{aligned}$$

   Sostituendo $|\Psi'\rangle = U|\Psi\rangle$ e $\left\langle \tilde{\Psi}' \right| = \left\langle \tilde{\Psi} \right| U^\dagger$, si ottiene, poiché U é unitaria,

   $$\left\langle \tilde{\Psi}' \middle| \Psi' \right\rangle = \left\langle \tilde{\Psi} \right| U^\dagger U |\Psi\rangle = \left\langle \tilde{\Psi} \middle| \Psi \right\rangle,$$

   e quindi

   $$(\langle\tilde{\varphi}|\varphi\rangle)(\left\langle \tilde{\beta}' \middle| \beta' \right\rangle - 1) = 0.$$

   Dall'ipotesi che $\langle\tilde{\varphi}|\varphi\rangle \neq 0$ concludiamo che $|\beta'\rangle$ e $\left|\tilde{\beta}'\right\rangle$ sono stati identici e quindi non distinguibili da nessuna misurazione.

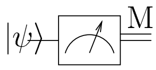

Figure 1: Simbolo usato nei circuiti per indicare la misura di un qubit nella base computazionale

2. Se gli stati $|\varphi\rangle$ e $|\tilde{\varphi}\rangle$ sono ortogonali il ragionamento precedente non porta a nessuna conclusione. In generale, si puó trovare una trasformazione U che permette di distinguere i due stati del sistema A attraverso una misurazione del sistema ausiliario B. Una possibilitá é applicare il `CNOT` dopo aver opportunemente scelto le basi.

Nei circuiti quantistici "misurare" costituisce quasi sempre la parte finale del circuito e viene spesso usata come un'operazione implicita. Negli esempi di circuiti che abbiamo studiato abbiamo usato il simbolo in figura 1 per denotare *misure proiettive*, cioé descritte mediante operatori di proiezione, P_m, ortogonali e tali che $\sum_m P_m = 1$. Per questo tipo di osservabile definito da $\sum_m mP_m$ abbiamo usato la frase "misurare nella base $\{|m\rangle\}_m$", dove la base é una base ortonormale che di solito corrisponde alla base computazionale.

Esistono due principi che descrivono due importanti proprietá della misurazione in un circuito quantistico. Il primo principio riguarda l'interscambiabilitá tra operazioni condizionali classiche e quantistiche.

Principio di misurazione deferita Se i risultati di un'operazione di misura sono usati in uno stadio intermedio di un circuito quantistico per operazioni di controllo classiche, allora queste operazioni possono essere sostituite da operazioni di controllo quantistiche e l'operazione di misura puó essere spostata dallo stadio intermedio allo stadio finale del circuito.

Un esempio tipico dove misurazioni avvengono nel mezzo di una computazione quantistica per ottenere dei bit classici usati per controllare successive operazioni quantistiche é il circuito per il teletrasporto quantistico.

Esercizio 1.2 *Trasformare il circuito quantistico per il teletrasporto in figura 10 della lezione 2 in un circuito dove le operazioni di misura sono eseguite alla fine e dimostrare l'equivalenza dei due circuiti. (Ovviamente il circuito trasformato non potrá piú essere usato per teletrasportare informazione classica tra Alice e Bob!).*

Principio di misurazione implicita Ogni linea (qubit) di un circuito quantistico che non termina con un operazione di misura si puó assumere come terminata da una operazione di misura implicita.

Intuitivamente questo principio afferma che in un circuito quantistico formato per esempio da due soli qubits, le statistiche che osserviamo dalla misura del primo qubit non sono influenzate da un'eventuale misura effettuata anche sul secondo qubit.