Quantum Computing

Alessandra Di Pierro

Appunti del corso - A.A. 2001-2002

Lezione 3: Introduzione generale

1 Porte logiche a più qubits

Le operazioni su registri quantistici di due o più qubits sono necessarie per descrivere le trasformazioni di stati composti e in particolare dei cosiddetti stati *entangled*. Abbiamo visto che non sempre un registro di due qubits può essere decomposto nel prodotto tensore dei singoli qubits componenti. Di conseguenza non possiamo in questi casi simulare un'operazione sui due qubits mediante operazioni su ciascun qubit componente.

Anche le operazioni su registri di qubits corrispondono a operazioni unitarie come nel caso di un singolo qubit.

Le più importanti porte logiche che implementano operazioni su due bits classici sono le porte `AND`, `OR`, `XOR`, `NAND` e `NOR`. Le porte `NOT` e `AND` formano un insieme *universale*, cioè qualsiasi funzione booleana si può realizzare mediante una combinazione di queste due operazioni. Per lo stesso motivo, il `NAND` costituisce un insieme universale. Nota che `XOR` da solo o anche insieme con `NOT` non è universale: poichè preserva la parità totale dei bits, solo un sottinsieme delle funzioni booleane sono rappresentabili mediante questa operazione.

L'analogo quantistico di `XOR` è la porta `CNOT` (controlled-`NOT`) che opera su due qubits: il primo è chiamato qubit di *controllo* e il secondo è il qubit *target*. Se il controllo è zero allora il target è lasciato inalterato; se il controllo è uno, allora il target viene negato, cioè:

$$|00\rangle \mapsto |00\rangle\,, |01\rangle \mapsto |01\rangle\,, |10\rangle \mapsto |11\rangle\,, |11\rangle \mapsto |10\rangle\,.$$

Equivalentemente, `CNOT` si può vedere come

$$|A, B\rangle \mapsto |A, B \oplus A\rangle\,,$$

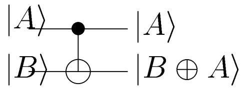

Figure 1: Porta `CNOT`

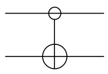

Figure 2: Variante della porta `CNOT`

dove A è il qubit di controllo, B è il target e $\oplus$ è la somma modulo 2, cioè l'operazione classica `XOR`.

La porta `CNOT` è rappresentata graficamente dal circuito in Figura 1.

La reppresentazione come matrice unitaria è:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

dove la prima colonna descrive la trasformazione del vettore della base computazionale $|00\rangle$, la seconda quella del vettore $|01\rangle$, la terza di $|10\rangle$ e la quarta di $|11\rangle$.

Esercizio 1.1 *Considera un'operazione analoga al* `CNOT` *dove il target è negato se il qubit di controllo è zero anzicchè uno. Questa opearzione è rappresentata come in Figura 2. Qual'è la sua rappresentazione matriciale?*

È importante osservare che il `CNOT`, come tutte le trasformazioni unitarie, è invertibile: dall'output si può sempre ottenere l'input. Questo non è vero per le porte logiche `XOR` e `NAND`: in generale le operazioni classiche sono *irreversibili.*

La porta `CNOT` e le porte a un qubit rappresentano i prototipi di tutte le porte logiche quantistiche. Infatti, mostreremo in seguito l'universalità di queste operazioni.

2 Circuiti quantistici

Un semplice esempio di circuito quantistico è dato in Figura 3. Il circuito realizza lo scambio degli stati di due qubits. Dato in input il registro di due qubits $|a, b\rangle$, viene effettuato un `CNOT` con qubit di controllo a. Come

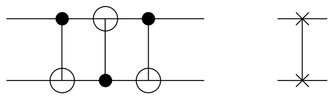

Figure 3: Circuito che scambia due qubits e simbolo schematico

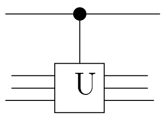

Figure 4: Porta controlled-U

risultato b viene rimpiazzato da $a \oplus b$. Quest'ultimo viene preso come controllo di un secondo `CNOT` con target a. L'effetto è che a viene sostituito da $a \oplus (a \oplus b) = b$. Un ultimo `CNOT` con controllo b e target $a \oplus b$ realizza infine lo scambio rimpiazzando $a \oplus b$ con a. Data una qualsiasi operazione unitaria U su n qubits, si può definire il circuito *controlled-U* come la naturale estensione della porta `CNOT` (cf. Figura 4). La linea con il pallino nero indica il qubit di controllo, mentre i qubits target sono gli n inputs di U. Secondo questa convenzione il *controlled-*`NOT` non è altro che un *controlled-U* con $U = X$.

Un'altra operazione importante è rappresentata dal simbolo in Figura 5 e consiste nella misurazione di un qubit $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Come sappiamo il risultato è un bit classico M (indicato con una doppia linea) che sarà 0 oppure 1 con probabilità rispettivamente $|\alpha|^2$ e $|\beta|^2$.

2.1 No-cloning

È possibile costruire un circuito che fa la copia di un qubit? Si potrebbe pensare di utilizzare un `CNOT` con qubit di controllo contenente il qubit $|x\rangle$ da copiare e il target posto inizialmente a $|0\rangle$. I risultato sarebbe la copiatura di x nel target. In realtà questo è vero per bit classici (o per gli stati della base computazionale) ma non per un generico qubit $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$. Infatti, consideriamo il circuito in Figura 6, costituito da un `CNOT` che ha come input i qubits $|\psi\rangle$ (controllo) e $|0\rangle$ (target), cioè il registro $|\psi\rangle\,|0\rangle$.

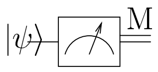

Figure 5: Simbolo di circuito per la misurazione

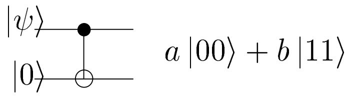

Figure 6: Circuito quantistico per "copiare" un qubit

Il nostro obiettivo è ottenere il risultato $|\psi\rangle\,|\psi\rangle$. Osserviamo che

$$|\psi\rangle\,|\psi\rangle = a^2\,|00\rangle + ab\,|01\rangle + ab\,|10\rangle + b^2\,|11\rangle\,.$$

Questo stato è in generale diverso dal risultato del nostro circuito $a\,|00\rangle + b\,|11\rangle$ a meno che $ab = 0$. Quindi questo circuito non effettua la copia di un qubit. In generale, l'impossibilità di copiare un qubit è una proprietà dei sistemi quantistici nota come teorema del *no cloning*:

Teorema 2.1 *Non esiste una trasformazione unitaria M tale che $M\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$, per tutti gli stati $|\psi\rangle$.*

Dimostrazione Supponiamo che esista M tale che $M\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$, per tutti i qubits $|\psi\rangle$. Allora possiamo scegliere due qubits $|\psi\rangle$ e $|\phi\rangle$ tali che $0 < \langle\psi,\phi\rangle < 1$. Ad esempio, si può prendere $|\psi\rangle = |0\rangle$ e $|\phi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Allora otteniamo che

$$M\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle \;\text{ e }\; M\,|\phi\rangle\,|0\rangle = |\phi\rangle\,|\phi\rangle\,.$$

Facciamo ora il prodotto scalare delle due equazioni. Siccome M è unitaria e quindi preserva i prodotti scalari (cf. Esercizio $A.8$ della Lezione 2), e per la proprietà distributiva del prodotto tensore rispetto al prodotto scalare (cf. Esercizio $A.4$ della Lezione 1) otteniamo che

$$\langle\psi,\phi\rangle\,\langle\psi,\phi\rangle = \langle\psi,\phi\rangle\,\langle 0,0\rangle = \langle\psi,\phi\rangle\,,$$

contraddicendo l'ipotesi $0 < \langle\psi,\phi\rangle < 1$. Quindi M non può esistere.

2.2 Esempi di circuiti quantistici

Descriviamo due circuiti un po' più complicati di quelli visti precedentemente: il primo permette di trasformare i quattro stati computazionali di due qubits in altrettanti stati che sono detti *stati di Bell* o *coppie EPR*; il secondo usa questi stati per realizzare il *teletrasporto* di un qubit. Questi due esempi mostrano come costruire stati computazionali che non hanno alcuna controparte classica e usarli per dar luogo a fenomeni paradossali secondo le leggi della fisica classica. Tali stati sono quelli che abbiamo chiamato *entangled*.

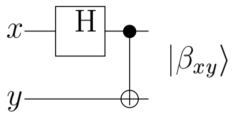

Figure 7: Circuito quantistico per la creazione degli stati di Bell

2.2.1 Stati di Bell

Abbiamo visto che la porta `CNOT` può essere usata per creare stati che sono entangled. Il circuito in Figura 7 genera per ogni stato della base computazionale $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ un particolare stato entangled. Questi stati, che indichiamo con $\beta_{00}, \beta_{10}, \beta_{01}, \beta_{11}$, sono chiamati stati di Bell o EPR da Bell Einstein Podolsky e Rosen che per primi ne scoprirono le straordinarie proprietà. In particolare, Einstein Podolsky e Rosen usarono questi stati in un esperimento che nelle loro intenzioni doveva dimostrare che la meccanica quantistica non era in grado di dare una descrizione completa della realtà. Il paradosso che veniva fuori da questo esperimento era che l'interazione tra queste coppie di stati quantistici dava luogo a un fenomeno che violava i principi fondamentali della teoria della relatività. La spiegazione "classica" che essi proponevano fu successivamente smentita da Bell.

Il circuito trasforma il primo qubit in una sovrapposizione che viene poi usata come input di controllo per `CNOT`. Il target viene quindi invertito solo quando il controllo è 1. Pertanto i vettori in input vengono trasformati come segue:

$$
\begin{array}{lcl}
|00\rangle & \mapsto & |\beta_{00}\rangle \equiv (|00\rangle + |11\rangle / \sqrt{2}) \\
|01\rangle & \mapsto & |\beta_{01}\rangle \equiv (|01\rangle + |10\rangle / \sqrt{2}) \\
|10\rangle & \mapsto & |\beta_{10}\rangle \equiv (|00\rangle - |11\rangle / \sqrt{2}) \\
|11\rangle & \mapsto & |\beta_{11}\rangle \equiv (|01\rangle - |10\rangle / \sqrt{2})
\end{array}
$$

2.2.2 Teletrasporto quantistico

Il teletrasporto quantistico è una tecnica per trasportare stati quantistici da un posto ad un altro anche in assenza di canali di comunicazione che collegano il punto da cui lo stato viene mandato al punto in cui viene ricevuto. Questa tecnica è stata scoperta nel 1993 e la sua validità è stata poi confermata da vari risultati sperimentali. Per capire il tipo di problemi che permette di risolvere, immaginiamo una situazione in cui una persona che

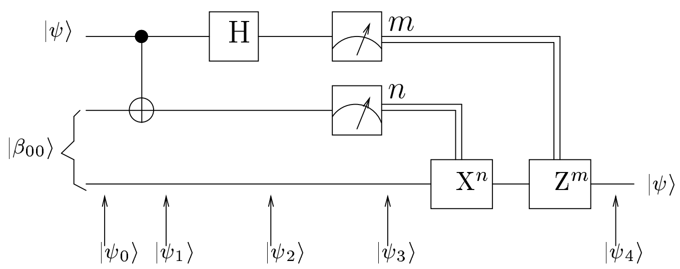

Figure 8: Circuito quantistico per il teletrasporto di un qubit

chiamiamo Alice deve far conoscere lo stato di un qubit ad un'altra persona che chiameremo Bob. Alice non conosce lo stato del qubit e per il teorema del no-cloning sappiamo che non le è possibile farne una copia. Inoltre Alice può solo mandare a Bob informazione classica, cioè i valori 0 e 1 di un bit classico. In questa situazione sembrebbe impossibile tarsmettere il qubit a Bob. Vediamo come ciò è possibile grazie alle proprietà degli stati entangled. L'ipotesi fondamentale è che Bob e Alice possiedono ciascuno un qubit di una coppia EPR generata precedentemente. Alice può operare sul suo qubit e Bob può fare altrettanto sulla sua parte della coppia EPR. Il circuito in Figura 8 illustra come avviene la trasmissione di un qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ di cui si ignorano le ampiezze α e β, da parte di Alice a Bob. Lo stato di input del circuito è $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$.

Alice combina $|\psi\rangle$ con la sua metà della coppia EPR e misura i suoi due qubits dopo aver applicato le porte `CNOT` e Hadamard. I due bit che ottiene dopo la misurazione vengono mandati attraverso un canale di comunicazione classico a Bob, il quale sarà in grado di ricostruire lo stato $|\psi\rangle$ sfruttando l'informazione classica ricevuta da Alice e la sua metà della coppia EPR.

Nel circuito in figura, le prime due linee corrispondono ai qubits usati da Alice, mentre l'ultima linea corrisponde al qubit posseduto da Bob. L'input è

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)],$$

dove lo stato $|\beta_{00}\rangle \equiv (|00\rangle + |11\rangle/\sqrt{2})$ occupa il secondo qubit di Alice e il qubit di Bob. Come risultato di `CNOT` applicato ai suoi due qubits, Alice ottiene

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)].$$

Viene quindi applicato Hadamard al primo qubit, $|\psi\rangle$, ottenendo

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)],$$

che si può scrivere equivalentemente come

$$|\psi_2\rangle = \frac{1}{2}[|00\rangle\,(\alpha\,|0\rangle+\beta\,|1\rangle)+|01\rangle\,(\alpha\,|1\rangle+\beta\,|0\rangle)+|10\rangle\,(\alpha\,|0\rangle-\beta\,|1\rangle)+|11\rangle\,(\alpha\,|1\rangle-\beta\,|0\rangle)].$$

A questo punto Alice misura i suoi due qubits ottenendo una delle quattro coppie di bits:

$$00\ 01\ 10\ 11.$$

Per effetto della misurazione anche il qubit di Bob collasserà nello stato corrispondente al risultato della misurazione, cioè:

$$\begin{array}{rcl} 00 & \mapsto & \alpha\,|0\rangle + \beta\,|1\rangle \\ 01 & \mapsto & \alpha\,|1\rangle + \beta\,|0\rangle \\ 10 & \mapsto & \alpha\,|0\rangle - \beta\,|1\rangle \\ 11 & \mapsto & \alpha\,|1\rangle - \beta\,|0\rangle \end{array}$$

Nella figura questo stato è indicato con $|\psi_3\rangle$.

Alice comunica i due bit mn ottenuti a Bob mediante un canale classico. Bob è ora in grado di ottenere il qubit $|\psi\rangle$ applicando al suo qubit il circuito $X^n Z^m$, dove

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$