Quantum Computing

Alessandra Di Pierro

Introduzione ai circuiti quantistici

1 Porte logiche quantistiche

Abbiamo studiato la descrizione quantistica degli stati di una computazione. Vediamo ora come questi stati evolvono dando luogo ad una computazione quantistica.

Analogamente ai computer classici, un computer quantistico è formato da circuiti quantistici costituiti da *porte logiche quantistiche* elementari.

Nel caso classico esiste un'unica porta logica (non banale) a un bit, la porta `NOT`, che implementa l'operazione logica di negazione definita mediante una tabella di verità in cui $1 \to 0$ e $0 \to 1$.

Per definire un'operazione analoga su un qubit, non possiamo limitarci a stabilire la sua azione sugli stati di base $|0\rangle$ e $|1\rangle$, ma dobbiamo specificare anche come deve essere trasformato un qubit che si trova in una sovrapposizione degli stati $|0\rangle$ e $|1\rangle$. Intuitivamente, il `NOT` dovrebbe scambiare i ruoli dei due stati fondamentali e trasformare $\alpha|0\rangle + \beta|1\rangle$ in $\beta|0\rangle + \alpha|1\rangle$. Chiaramente $|0\rangle$ si trasformerebbe in $|1\rangle$ e $|1\rangle$ in $|0\rangle$. L'operazione che implementa questo tipo di trasformazione è un'operazione *lineare* e, come vedremo, questa è una proprietà generale della meccanica quantistica che si giustifica sperimentalmente. Un modo conveniente per rappresentare operazioni lineari è per mezzo di matrici.

1.1 Rappresentazione di operatori lineari

Una funzione $L : \mathbb{C}^2 \mapsto \mathbb{C}^2$ si dice lineare se per ogni $a_1, a_2 \in \mathbb{C}$ e $v_1, v_2 \in \mathbb{C}^2$:

$$L(a_1v_1 + a_2v_2) = a_1L(v_1) + a_2L(v_2).$$

Dato un vettore $u \in \mathbb{C}^2$, il duale di u è la funzione lineare $L_u : \mathbb{C}^2 \mapsto \mathbb{C}$ definito da $L_u(w) = (u, w) = u^\dagger w$. Spesso si identifica L_u con $u^\dagger$. Nella notazione di Dirac il duale di un vettore $|\psi\rangle$ è denotato da $\langle\psi|$ e il prodotto scalare di $|\psi\rangle$ e $|\phi\rangle$ da $\langle\psi|\phi\rangle$. Per vettori a norma 1 il significato di $L_u(w) = \langle u|w\rangle$ è la proiezione di w nella direzione di u.

Esercizio 1.1 *Dimostrare che la somma di due funzioni lineari è lineare.*

Esercizio 1.2 *Dimostrare che la funzione lineare* $|\psi\rangle\langle\phi| : \mathbb{C}^2 \mapsto \mathbb{C}^2$ *definita da* $|\psi\rangle\langle\phi|(|x\rangle) = \langle\phi|x\rangle|\psi\rangle$ *è lineare.*

La matrice di rappresentazione di una funzione lineare L nella base computazionale $|0\rangle$ e $|1\rangle$ si definisce a partire da $L(|0\rangle)$ e $L(|1\rangle)$ come segue. Supponiamo che

$$L(|0\rangle) = a_{11}|0\rangle + a_{21}|1\rangle$$

e

$$L(|1\rangle) = a_{12}|0\rangle + a_{22}|1\rangle .$$

Allora possiamo scrivere L come

$$L = a_{11}|0\rangle\langle 0| + a_{21}|1\rangle\langle 0| + a_{12}|0\rangle\langle 1| + a_{22}|1\rangle\langle 1| .$$

La matrice

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

è la matrice di rappresentazione di L nella base computazionale $|0\rangle$ e $|1\rangle$.

1.1.1 Cambio di base

Il passaggio da una base ad un'altra è una trasformazione lineare la cui matrice si costruisce come segue. Supponiamo che i vettori $|\psi_1\rangle$ e $|\psi_2\rangle$ formino una base per $\mathbb{C}^2$ e che in tale base risulti $|0\rangle = b_{11}|\psi_1\rangle + b_{21}|\psi_2\rangle$ e $|1\rangle = b_{12}|\psi_1\rangle + b_{22}|\psi_2\rangle$. Allora la matrice del cambio di base è data da:

$$B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}.$$

Il vettore con rappresentazione $(\alpha, \beta)^T$ nella base $|0\rangle$ e $|1\rangle$, avrà coordinate $B(\alpha, \beta)^T$ rispetto alla base $|\psi_1\rangle$ e $|\psi_2\rangle$.

Esempio 1.3 *Considera la base formata dai due qubits* $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ *e* $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. *La matrice del cambio di base da* $|0\rangle$, $|1\rangle$ *a* $|+\rangle$, $|-\rangle$ *è data da*

$$B = \sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Esercizio 1.4 *Verificare che la rappresentazione di L nella nuova base è BAB^{-1}*

Esercizio 1.5 *Dimostrare che la rappresentazione di* `NOT` *nella base $|0\rangle$ e $|1\rangle$ è la matrice*

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

Qual è la sua rappresentazione nella base $|+\rangle$, $|-\rangle$?

1.2 Matrici unitarie

Data una matrice $n \times m$ A, la trasposta A^T è definita da $(A^T)_{ij} = (A)_{ji}$. La coniugata A^* di A è la matrice $(A^*)_{ij} = (A)^*_{ij}$. La matrice aggiunta $A^\dagger$ di A è la matrice $A^\dagger = (A^T)^*$.

Una matrice A è detta unitaria se $A^\dagger = A^{-1}$, dove A^{-1} è l'inversa di A, cioè $AA^{-1} = I$ (I è la matrice identità, $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$).

Esercizio 1.6 *Dimostrare che le matrici*

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \; Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ e } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

sono unitarie. X, Y e Z sono dette le matrici di Pauli.

Esercizio 1.7 *Dimostrare che*

$$\langle u|Av\rangle = \langle A^\dagger u|v\rangle.$$

Dedurre la seguente proprietà delle matrici unitarie: M è unitaria se e solo se preserva i prodotti scalari, cioè se e solo se $\langle Mu|Mv\rangle = \langle u|v\rangle$, per ogni $u, v \in \mathbb{C}^2$.

1.3 Porte logiche quantistiche a un qubit

La matrice corrispondente al `NOT` quantistico è chiamata per motivi storici X ed è definita da:

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

Si può infatti verifcare che l'applicazione di X a un qubit $\alpha|0\rangle + \beta|1\rangle$ (scritto in notazione vettoriale) è:

$$X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix}.$$

In generale un'operazione su un singolo qubit può essere specificata da una matrice 2×2. Tuttavia non tutte le matrici 2×2 definiscono operazioni "lecite" su qubits. Ricordiamo che la condizione di normalizzazione richiede che $|\alpha^2 + \beta^2| = 1$ in qualsiasi stato quantistico $\alpha|0\rangle + \beta|1\rangle$. La stessa condizione deve valere anche per lo stato che si ottiene dopo aver effettuato l'operazione. La proprietà delle matrici che garantisce la trasformazione di un vettore unitario in un vettore che è ancora unitario è l'*unitarietà*.

Teorema 1.8 *Una funzione lineare trasforma un qubit in un qubit (cioè preserva vettori normalizzati) se e solo se è unitaria.*

Dimostrazione Esercizio.

Contrariamente al caso classico in cui possiamo definire una sola operazione non banale su un singolo bit, nel caso quantistico esistono molte operazioni non banali su un singolo qubit. Oltre al `NOT` due operazioni importanti che useremo in seguito sono la porta Z e la porta di *Hadamard*:

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

che agisce solo sulla componente $|1\rangle$ scambiandone il segno,

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Quest'ultima operazione è una delle più utili e viene usata molto spesso nella definizione di circuiti quantistici. Il suo effetto è quello di trasformare uno stato base in una sovrapposizione che risulta, dopo una misurazione nella base computazionale, essere 0 oppure 1 con uguale probabilità. Ad esempio, applicando H a $|0\rangle$ si ottiene:

$$H \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

cioè lo stato $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. L'effetto di H si può quindi vedere come un `NOT` eseguito a metà in modo che lo stato risultante non è ne' 0 ne' 1, bensì una sovrapposizione coerente dei due stati di base. Per questo motivo H viene spesso

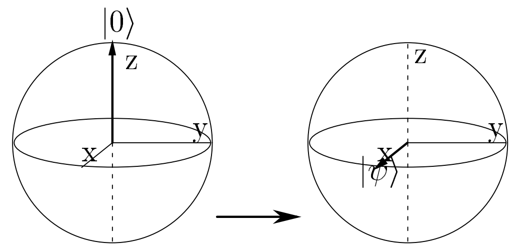

Figure 1: Visualizzazione della porta di Hadamard applicata all'input $|0\rangle$. L'output è $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$.

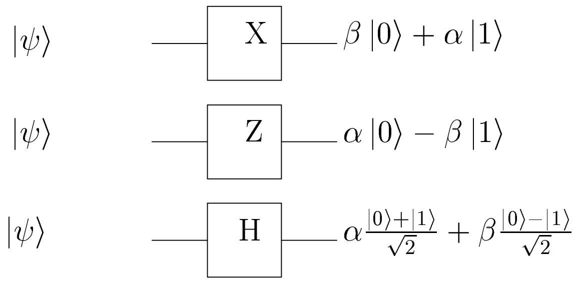

Figure 2: Le porte X, Z e H

chiamata la "radice quadrata di `NOT`". Nota che questa espressione ha un significato solo fisico! Da un punto di vista algebrico, H^2 *non* è la matrice X. Con un semplice calcolo si può infatti verificare che H^2 è l'identità e quindi applicando due volte H ad uno stato lo lascia inalterato.

Nella sfera di Bloch l'operazione H corrisponde ad una rotazione di $90°$ della sfera intorno all'asse y seguita da una riflessione attraverso il piano (x, y). In Figura 1 è illustrato l'effetto dell'applicazione di H al qubit $|0\rangle$. Si può provare a visualizzare l'effetto di H sul qubit $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Per effetto della rotazione e della successiva riflessione attraverso il piano x, y si otterrà nuovamente $|0\rangle$.

Le porte logiche a un qubit X, Z e H sono rappresentate graficamente come in Figura 2.

Le matrici X, Z e la matrice unitaria

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix},$$

sono chiamate *matrici di Paoli* e rappresentano rispettivamente le componenti x, z, y dello spin di un elettrone.

Si puó dimostrare che per ogni matrice unitaria U esistono numeri reali α, β, δ e γ tali che

$$U = \begin{bmatrix} e^{i(\alpha-\beta/2-\delta/2)}\cos(\frac{\gamma}{2}) & -e^{i(\alpha-\beta/2+\delta/2)}\sin(\frac{\gamma}{2}) \\ e^{i(\alpha+\beta/2-\delta/2)}\sin(\frac{\gamma}{2}) & e^{i(\alpha+\beta/2+\delta/2)}\cos(\frac{\gamma}{2}) \end{bmatrix}.$$

(esercizio)

1.4 Porte logiche quantistiche 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 la trasformazione

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

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 3.

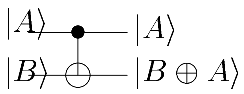

Figure 3: Porta `CNOT`

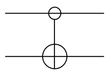

Figure 4: Variante della porta `CNOT`

La rappresentazione 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 1.9 *Considera un'operazione analoga al* `CNOT` *dove il target è negato se il qubit di controllo è zero anzicchè uno. Questa operazione è rappresentata come in Figura 4. Qual è la matrice che la rappresenta?*

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 5. 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 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

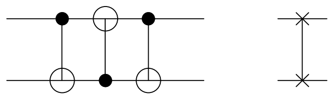

Figure 5: Circuito che scambia due qubits e simbolo schematico

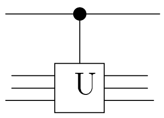

Figure 6: Porta controlled-U

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 6). 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 7 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 $|0\rangle$. Il 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 8, costituito da un `CNOT` che ha come input i qubits $|\psi\rangle$ (controllo) e $|0\rangle$ (target), cioè il registro $|\psi\rangle |0\rangle$.

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

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

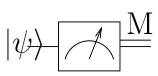

Figure 7: Simbolo di circuito per la misurazione

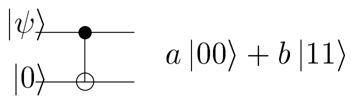

Figure 8: Circuito quantistico per "copiare" un qubit

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 ogni stato $|\psi\rangle$.*

Dimostrazione Supponiamo che esista M tale che $M\,|\psi\rangle\,|0\rangle = |\psi\rangle\,|\psi\rangle$, per ogni qubit $|\psi\rangle$. 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 membro a membro delle due equazioni. Siccome M è unitaria e quindi preserva i prodotti scalari (cf. Esercizio 1.7), e per la proprietà distributiva del prodotto tensore rispetto al prodotto scalare (cf. Esercizio 3.4 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*.

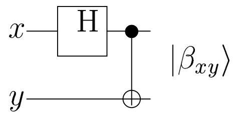

Figure 9: Circuito quantistico per la creazione degli stati di Bell

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 9 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:

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

2.2.2 Teletrasporto quantistico

Il teletrasporto quantistico è una tecnica per trasportare stati quantistici da un posto ad un altro sfruttando solo la trasmissione di bits classici. Questa tecnica è stata scoperta nel 1993 e la sua validità è stata poi confermata da vari risultati sperimentali. In un recente esperimento realizzato all'università di Ginevra e riportato sulla rivista *Nature* N. 421 del 30 gennaio 2003, è stato

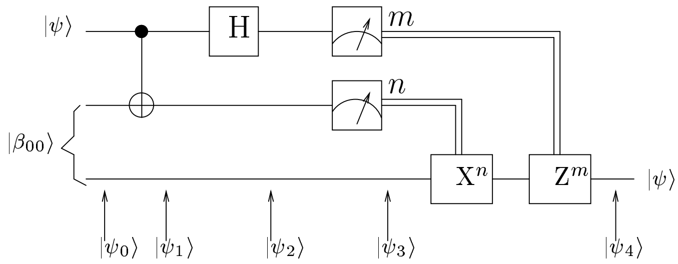

Figure 10: Circuito quantistico per il teletrasporto di un qubit

effettuato il teletrasporto di un qubit tra due laboratori posti a 55 metri di distanza e sfruttando un canale standard di telecomunicazione di 2 Km.

Per capire il tipo di problemi che permette di risolvere, immaginiamo una situazione in cui una persona che 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 10 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:

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

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

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