UNIVERSITÀ DEGLI STUDI DI NAPOLI
"FEDERICO II"

Scuola Politecnica e delle Scienze di Base

Area Didattica di Scienze Matematiche Fisiche e Naturali

Dipartimento di Fisica "Ettore Pancini"

Laurea Triennale in Fisica

L'entanglement e la trasmissione dell'informazione in meccanica quantistica

Relatori:
Massimo Taronna

Candidato:
Giacomo Marco
La Montagna
Matr. $N85001165$

Anno Accademico 2019/2020

Indice

Introduzione

Nel presente lavoro di tesi si vanno ad indagare gli aspetti caratterizzanti i sistemi quantistici aperti e uno degli effetti peculiari della meccanica quantistica, l'entanglement, con le sue conseguenze e applicazioni nella teoria dell'informazione quantistica, prestando particolare attenzione ai protocolli del Dense Coding e del Teletrasporto quantistico.

Verranno quindi presentati, inizialmente, i fondamenti matematici atti a descrivere formalmente i sistemi aperti approfondendo l'operatore di densità; sfruttando tale operatore si procederà a descrivere matematicamente l'entanglement e le differenze che nascono nella trattazione di stati puri e miscele.

Successivamente, con il formalismo introdotto, si affronterà il paradosso EPR discutendo le violazioni del principio di località per sistemi bipartiti e tripartiti. Inoltre, saranno descritti formalmente i protocolli di Dense Coding e del Teletrasporto: essi costituiscono le fondamenta dello scambio di informazioni nella computazione quantistica. Questa teoria vede le sue origini negli anni '80 quando il fisico Paul Benioff propose per la prima volta una *macchina di Turing quantistica* [4] e con l'articolo di Richard Feynmann [9] in cui egli presenta il computer quantistico come migliore strumento per simulare la realtà fisica dell'universo; col passare del tempo lo sviluppo della computazione quantistica è stato estremamente rapido proprio grazie alle numerose possibilità che offre di ridurre il grado di complessità di problemi di diffuso interesse. I due protocolli studiati si collocano, all'interno dell'evoluzione della teoria, come soluzione all'ostacolo rappresentato dal teorema *no cloning*, secondo il quale non è possibile creare l'esatta copia di uno stato quantistico senza modificare l'originale: senza poter copiare uno stato è estremamente complicato trasferire l'informazione contenuta in esso.

Infine verrà mostrata l'implementazione dei protocolli di Dense Coding e Teletrasporto quantistico sfruttando il framework *IBM Quantum Experience* che consente di programmare circuiti quantistici e simularne la loro esecuzione oppure eseguirli su computer quantistici veri e propri messi a disposizione della ricerca.

Capitolo 1

Sistemi aperti e operatore densità

1.1 Il Q-bit

La teoria dell'informazione quantistica si fonda su un'unità fondamentale di informazione chiamata, in analogia al bit classico, Q-bit (forma contratta per Quantum-bit). Matematicamente un Q-bit può essere modellizzato come un vettore in uno spazio di Hilbert $\mathcal{H}$ di dimensione due, che è il più "piccolo" spazio di Hilbert non banale. Un generico vettore di tale spazio può essere rappresentato come segue:

$$\psi = a\,|0\rangle + b\,|1\rangle\,, \tag{1.1}$$

dove $a, b \in \mathbb{C}$ soddisfano la condizione di normalizzazione $|a|^2 + |b|^2 = 1$ e non si è tenuto conto della fase globale, mentre $|0\rangle$ e $|1\rangle$ sono due versori indipendenti dello spazio e che per questo ne costituiscono una base.
Se inizialmente lo stato del sistema rappresentato dal Q-bit ψ è ignoto, una qualsiasi misura dello stesso, ovvero una proiezione dello stato su uno dei due vettori di base, produce come risultato $|0\rangle$ con probabilità $|a|^2$, $|1\rangle$ con probabilità $|b|^2$ e fissa il sistema in uno stato questa volta noto e diremo quindi che il sistema è stato $preparato$.

1.2 Operatore di densità

Si introduca adesso un secondo Q-bit. I due Q-bit, A e B, si dicono $correlati$ se lo stato del sistema da loro costituito può essere scritto come combinazione lineare del prodotto tensore tra i vettori di base dei rispettivi spazi di Hilbert $\mathcal{H}_A$ e $\mathcal{H}_B$:

$$\psi_{AB} = a\,|0\rangle_A \otimes |0\rangle_B + b\,|1\rangle_A \otimes |1\rangle_B\,. \tag{1.2}$$

In questa condizione se si effettua una misura proiettando ψ_{AB} su una sola delle due basi, ad esempio $\{|0\rangle_A\,, |1\rangle_A\}$, si ottiene con probabilità pari a $|a|^2$ lo stato

$|0\rangle_A \otimes |0\rangle_B$ e con probabilità $|b|^2$ lo stato $|1\rangle_A \otimes |1\rangle_B$.
Come si vede se, successivamente, si effettua una misura sulla base $\{|0\rangle_B, |1\rangle_B\}$ il risultato della misura sarà, con probabilità del 100%, $|0\rangle_B$ se precedentemente era stato misurato $|0\rangle_A$ oppure $|1\rangle_B$ se precedentemente era stato misurato $|1\rangle_A$: i risultati delle misure su $\{|0\rangle_A, |1\rangle_A\}$ e $\{|0\rangle_B, |1\rangle_B\}$ sono perfettamente $correlati$.
Si consideri, adesso, un generico osservabile **M** agente solo su uno dei due Q-bit, ad esempio A; esso può essere scritto come:

$$\mathbf{M} = \mathbf{M}_A \otimes \mathbf{I}_B \tag{1.3}$$

e il suo valore di aspettazione sarà:

$$\begin{aligned}\langle \mathbf{M} \rangle &= \langle \psi_{AB}| \, \mathbf{M}_A \otimes \mathbf{I}_B \, |\psi_{AB}\rangle \\ &= (a^* \langle 00| + b^* \langle 11|)\mathbf{M}_A \otimes \mathbf{I}_B (a\,|00\rangle + b\,|11\rangle) \\ &= (a^* \langle 0|_A + b^* \langle 1|_A)\mathbf{M}_A (a\,|0\rangle_A + b\,|1\rangle_A) + \\ &\quad + (a^* \langle 0|_B + b^* \langle 1|_B)\mathbf{I}_B (a\,|0\rangle_B + b\,|1\rangle_B) \\ &= |a|^2 \langle 0|_A \mathbf{M}_A |0\rangle_A + |b|^2 \langle 1|_A \mathbf{M}_A |1\rangle_A .\end{aligned} \tag{1.4}$$

Se si introduce l'operatore

$$\boldsymbol{\rho}_A = |a|^2 |0\rangle_A \langle 0|_A + |b|^2 |1\rangle_A \langle 1|_A , \tag{1.5}$$

il quale prende il nome di *operatore di densità* o *matrice di densità* parziale, è possibile notare che il risultato dell'equazione 1.4 può essere riscritto nella seguente forma:

$$\langle \mathbf{M} \rangle = tr\Big(\mathbf{M}_A \boldsymbol{\rho}_A\Big). \tag{1.6}$$

L'operatore di densità può essere interpretato come l'operatore che descrive l'insieme di tutti i possibili stati quantistici del sistema fisico, ognuno con la propria probabilità di occorrenza.

Se ora si paragona un sistema fisico costituito da un unico Q-bit con un sistema fisico costituito da due Q-bit, dei quali uno solo risulta accessibile al fine di effettuare una misura, iniziano ad apparire evidenti differenze. Per esempio, si consideri lo stato di un sistema fisico di $spin\ \frac{1}{2}$:

$$\psi = \frac{1}{\sqrt{2}}\Big(|\uparrow_z\rangle + |\downarrow_z\rangle \Big),$$

sovrapposizione coerente dei due stati $|\uparrow_z\rangle$ e $|\downarrow_z\rangle$. Se si misura lo spin lungo l'asse z essi risultano entrambi con probabilità $\frac{1}{2}$. Se invece si effettua una misura di $\boldsymbol{\sigma}_1$, si ottiene $|\uparrow_x\rangle$ con probabilità 1 in quanto ψ è autostato di $\boldsymbol{\sigma}_1$ di autovalore

1. Considerando un insieme probabilistico in cui gli stati $|\uparrow_z\rangle$ e $|\downarrow_z\rangle$ occorrono entrambi con probabilità $\frac{1}{2}$, se si misura lungo l'asse z, esso si rappresenta come:

$$\boldsymbol{\rho} = \frac{1}{2}\Big[\, |\uparrow_z\rangle \langle\uparrow_z| + |\downarrow_z\rangle \langle\downarrow_z| \,\Big] = \frac{1}{2}\boldsymbol{I}.$$

Dunque, la misura dello stato lungo la direzione x, ma come lungo una qualsiasi direzione $\hat{n}$ dello spazio, produrrà sempre risultato $\frac{1}{2}$:

$$\langle\hat{n}\rangle = tr\Big(\, |\hat{n}\rangle \langle\hat{n}|\, \boldsymbol{\rho}\Big) = \langle\hat{n}|\, \frac{1}{2}\boldsymbol{I}\, |\hat{n}\rangle = \frac{1}{2}.$$

La spiegazione di tale fenomeno va ricercata nel fatto che in questo caso il nostro sistema globale è costituito da due Q-bit e le misure vengono effettuate su una sua parte che costituisce dunque un sistema aperto. In tali condizioni gli stessi assiomi che reggono la meccanica quantistica perdono di validità in quanto formulati per un sistema chiuso; in particolare gli stati non sono in generale raggi, le misure non sono proiezioni ortogonali e l'evoluzione non è unitaria. Tuttavia va sottolineato che sistemi quantistici perfettamente chiusi sono solo ideali e dunque lo studio di sistemi aperti, i cui insiemi di probabilità sono descritti da operatori di densità, è di fondamentale importanza.

Il discorso è facilmente generalizzabile a un generico sistema quantistico bipartito $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. Una base di tale spazio è

$$\{|i\rangle_A \otimes |u\rangle_B\}$$

e dunque un generico stato sarà:

$$|\psi\rangle_{AB} = \sum_{i,u} a_{iu}\, |i\rangle_A \otimes |u\rangle_B\,. \tag{1.7}$$

Dove vale la condizione di normalizzazione $\sum_{iu} |a_{iu}|^2 = 1$. Procedendo in esatta analogia con il caso precedente, se si calcola il valore di aspettazione del generico osservabile **M** agente solo sul sottosistema A, si ottiene:

$$\begin{aligned}
\langle\mathbf{M}\rangle =& {}_{AB}\langle\psi|\, \mathbf{M}_A \otimes \boldsymbol{I}_B\, |\psi\rangle_{AB} \\
=& \sum_{j,v} a^*_{jv} \big({}_A\langle j| \otimes_B \langle v|\,\big) \big(\mathbf{M}_A \otimes \boldsymbol{I}_B\big) \sum_{i,u} a_{iu} \big(\, |i\rangle_A \otimes |u\rangle_B\,\big) \\
=& \sum_{i,j,u} a^*_{ju} a_{iu}\, \langle j|\, \mathbf{M}_A\, |i\rangle \\
=& \, tr\Big(\mathbf{M}_A \boldsymbol{\rho}_A\Big),
\end{aligned} \tag{1.8}$$

dove l'operatore di densità dell'insieme A è definito come:

$$\boldsymbol{\rho}_A = \sum_{i,j,u} a^*_{ju} a_{iu} \left|i\right\rangle \left\langle j\right| = tr_B\big(\left|\psi\right\rangle \left\langle\psi\right|\big); \tag{1.9}$$

ovvero l'operatore di densità dell'insieme A equivale alla *traccia parziale* dello stato sull'insieme B. La traccia parziale può essere interpretata come un operatore che mappa un vettore di $\mathcal{H}_A \otimes \mathcal{H}_B$ in $\mathcal{H}_A$:

$$tr_B\big(\mathbf{M}_{AB}\big) = \sum_u {}_B\left\langle u\right| \mathbf{M}_{AB} \left|u\right\rangle_B . \tag{1.10}$$

Dall'equazione 1.9 si possono dedurre in maniera immediata delle notevoli proprietà dell'operatore densità:

1. è autoaggiunto: $\boldsymbol{\rho}_A = \boldsymbol{\rho}_A^\dagger$;
2. è semidefinito positivo: $\forall \left|\phi\right\rangle , \left\langle\phi\right| \boldsymbol{\rho}_A \left|\phi\right\rangle = \sum_u \Big| \sum_i a_{iu} \left\langle\phi\right| \left|i\right\rangle \Big|^2 \geq 0$;
3. è a traccia unitaria: $tr\big(\boldsymbol{\rho}_A\big) = 1$.

L'operatore di densità è dunque diagonalizzabile, i suoi autovalori saranno non negativi e a somma 1. In forma diagonale esso si può scrivere come:

$$\boldsymbol{\rho}_A = \sum_a p_a \left|a\right\rangle \left\langle a\right| , \tag{1.11}$$

dove $\{\left|a\right\rangle\}$ è la base ortonormale che diagonalizza $\boldsymbol{\rho}_A$. Se tale base è costituita da un unico versore allora l'operatore di densità sarà un proiettore, ovvero $\boldsymbol{\rho}_A^2 = \boldsymbol{\rho}_A$ e lo stato si dirà $puro$, altrimenti prenderà il nome di $miscela$. L'operatore densità può essere quindi visto come una *miscela incoerente* di stati $\{\left|a\right\rangle\}$ ovvero la cui fase relativa non è sperimentalmente accessibile.

Quando tra due sistemi A e B si instaura una correlazione essi si dicono $entangled$. Se inizialmente si era in possesso di una sovrapposizione coerente di stati di uno dei due insiemi, ad esempio A, l'entanglement causa la perdita della coerenza di tale sovrapposizione, o, in altre parole, fa sì che la fase reciproca di alcuni degli stati di A, precedentemente nota, non sia più accessibile effettuando misure solo sul sistema A.

1.3 Stati separabili e non separabili

Uno stato entangled è anche detto *non separabile* in quanto non può essere scritto come $\psi_{AB} = \psi_A \otimes \psi_B$, se invece tale scrittura è possibile lo stato è detto

separabile. Un metodo per verificare la separabilità di uno stato è quello di studiarne la sua *decomposizione di Schmidt*. Essa costituisce una particolare decomposizione a valori singolari che a sua volta è una sorta di generalizzazione, a matrici non quadrate, della decomposizione spettrale. Una generica decomposizione di Schmidt dello stato considerato, normalizzato, può essere scritta come:

$$|\psi\rangle_{AB} = \sum_{k=1}^{r} \sqrt{\lambda_k}\, |\chi_k\rangle_A \otimes |\phi_k\rangle_B \,, \tag{1.12}$$

dove:

$$|\psi\rangle_{AB} \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B, \quad |\chi\rangle_A \in \mathcal{H}_A, \quad |\phi\rangle_B \in \mathcal{H}_B,$$
$$r = min\{dim\mathcal{H}_A, dim\mathcal{H}_B\} \quad \text{e} \quad \sum_{k=1}^{r} \lambda_k = 1.$$

Dalla condizione di normalizzazione sui coefficienti risulta immediato dedurre che condizione necessaria e sufficiente alla separabilità di uno stato sia possedere r, *rango di Schmidt*, uguale a 1. In questo senso si può affermare che il rango di Schmidt "misura" la separabilità di uno stato.

Richiamando la definizione di operatore di densità 1.9, se si scrive lo stato $|\psi\rangle \in \mathcal{H}$ nella sua decomposizione di Schmidt si ottiene:

$$\begin{aligned}
\boldsymbol{\rho}_A &= tr_B\big(\, |\psi\rangle \langle\psi| \,\big) \\
&= \sum_{u}^{d_B} {}_B\langle u| \sum_{k=1}^{r} \big(\sqrt{\lambda_k}\, |\chi_k\rangle_A \otimes |\phi_k\rangle_B\big)\big(\sqrt{\lambda_k}\, \langle\chi_k|_A \otimes \langle\phi_k|_B\big)\, |u\rangle_B \\
&= \sum_{k=1}^{r}\sum_{u}^{d_B} \lambda_k \big(\, |\chi_k\rangle_A \langle\chi_k| \otimes_B \langle u|\phi_k\rangle_B \langle\phi_k|u\rangle_B \,\big) \\
&= \sum_{k=1}^{r} \lambda_k\, |\chi_k\rangle_A \langle\chi_k| \,,
\end{aligned} \tag{1.13}$$

dove si può notare che il quadrato dei coefficienti della decomposizione a valori singolari dello stato ψ sono gli autovalori dell'operatore $\boldsymbol{\rho}_A$. Procedendo in maniera analoga per B si giunge a

$$\boldsymbol{\rho}_B = tr_A\big(\, |\psi\rangle \langle\psi| \,\big) = \sum_{k=1}^{r} \lambda_k\, |\phi_k\rangle_B \langle\phi_k| \,, \tag{1.14}$$

da cui si evince immediatamente che i due operatori di densità posseggono lo stesso spettro. Tale proprietà risulta valida soltanto nell'ipotesi in cui ψ sia uno stato puro e non una miscela a sua volta in quanto si è fatto implicito utilizzo della relazione $\boldsymbol{\rho} = |\psi\rangle \langle\psi|$ e non $\boldsymbol{\rho} = \sum_i p_i\, |\psi_i\rangle \langle\psi_i|$.

La decomposizione di Schmidt ci permette anche di giungere alla conclusione che l'entanglement non può essere creato se i due sistemi non entrano in contatto. Infatti per creare una correlazione è necessario applicare globalmente trasformazioni unitarie in quanto trasformazioni unitarie locali non mutano il rango di Schmidt dello stato.

1.4 Distanza tra due stati

Definiamo *fedeltà* di due stati quella grandezza che ne misura la loro distinguibilità. Per stati puri $|\psi\rangle$ e $|\phi\rangle$ essa corrisponde con la norma quadra della loro sovrapposizione:

$$F(\psi, \phi) = |\langle\psi|\phi\rangle|^2. \tag{1.15}$$

Quando si trattano invece delle miscele descritte dagli operatori densità $\boldsymbol{\rho}$ e $\boldsymbol{\sigma}$ la fedeltà tra esse si definisce come:

$$F(\boldsymbol{\rho}, \boldsymbol{\sigma}) \equiv \left(tr\sqrt{\boldsymbol{\rho}^{\frac{1}{2}}\boldsymbol{\sigma}\boldsymbol{\rho}^{\frac{1}{2}}} \right)^2 = \left|\left| \boldsymbol{\rho}^{\frac{1}{2}}\boldsymbol{\sigma}^{\frac{1}{2}} \right|\right|_1^2 \tag{1.16}$$

e può essere espressa nei termini della norma L^1 - $||\mathbf{A}||_1 = tr\sqrt{\mathbf{A}^\dagger\mathbf{A}}$ - dei due operatori di densità.

Fisicamente, si può interpretare la fedeltà come la probabilità che hanno due stati di coinciderere completamente. Un risultato importante da evidenziare sulla fedeltà è la sua monotonia:

$$F(\boldsymbol{\rho}_{AB}, \boldsymbol{\sigma}_{AB}) \leq F(\boldsymbol{\rho}_A, \boldsymbol{\sigma}_A), \tag{1.17}$$

ovvero che calcolare la fedeltà tra due stati su un sottosistema fornisce una distinguibilità dei due minore o al più uguale a quando la si possa stimare sul sistema completo.

Capitolo 2

Entanglement e trasferimento informazioni

2.1 Stati di Bell e paradosso EPR

Dato un qualsiasi sistema bipartito AB è possibile definire uno stato massimamente entangled se i coefficienti di Schmidt possono essere scritti nella forma

$$\lambda_i = \frac{1}{d} \qquad \text{con} \quad d = min\{dim\mathcal{H}_{\mathcal{A}}, dim\mathcal{H}_{\mathcal{B}}\}.$$

Ciò comporta che l'operatore di densità parziale risulta essere

$$\boldsymbol{\rho_A} = tr_B\big(\,|\psi\rangle\,\langle\psi|\,\big) = \frac{\mathbf{I}_A}{d}, \tag{2.1}$$

allo stesso modo per $\boldsymbol{\rho_B}$. Per un sistema bipartito di due Q-bit A e B, in cui $d = 2$, la precedente relazione porta a concludere che uno stato massimamente entangled ha l'operatore di densità parziale proporzionale a $\frac{\mathbf{I}}{2}$. Un particolare set di tali stati massimamente entangled è:

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(\,|01\rangle \pm |10\rangle\,\big); \tag{2.2}$$

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}\big(\,|00\rangle \pm |11\rangle\,\big). \tag{2.3}$$

Tali stati, detti *stati di Bell*, costituiscono una base dello spazio $\mathcal{H}_A \otimes \mathcal{H}_B$. Una peculiarità di tali stati è che se si separano i due Q-bit e si agisce con matrici di Pauli localmente su di essi è possibile trasformare uno stato di Bell in un altro stato di Bell. Ad esempio se si opera solo sul Q-bit B si ha:

$$|\phi^-\rangle = \big(\mathcal{I}_A \otimes \boldsymbol{\sigma_B^1}\big)\,|\psi^-\rangle\,, \quad |\psi^+\rangle = \big(\mathcal{I}_A \otimes \boldsymbol{\sigma_B^3}\big)\,|\psi^-\rangle\,, \quad |\phi^+\rangle = \big(\mathcal{I}_A \otimes \boldsymbol{\sigma_B^2}\big)\,|\psi^-\rangle\,.$$

In uno stato massimamente entangled si dice che l'informazione è nascosta nel senso che, se si separano i due sistemi A e B, una volta instaurato l'entanglement, se non si conosce preventivamente lo stato iniziale risulta impossibile dedurlo tramite misure locali su A o su B, ovvero senza ricongiungere i due sistemi. Al contrario, se si conosce lo stato iniziale, misurando uno dei due sistemi è possibile dedurre lo stato dell'altro di conseguenza.

Per maggiore fluidità di narrazione si considerino due esperti sperimentatori, Alice e Bob, distanti tra loro, rispettivamente in possesso dei sistemi A e B precedentemente entangled. Supposto che lo stato del sistema completo sia $\psi^- = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$, se Alice misura $\boldsymbol{\sigma}^3_A$ otterrà $|0\rangle_A$ o $|1\rangle_A$ con probabilità $\frac{1}{2}$ in quanto $|0\rangle$ o $|1\rangle$ sono autostati di $\boldsymbol{\sigma}^3$. Dunque se Alice è a conoscenza dello stato del sistema completo può, dopo la sua misura, inferire con certezza riguardo lo stato di Bob nella medesima base. Tuttavia se si considerano come base di A o B la coppia di stati $|\pm\rangle = \frac{|0\rangle \pm |1\rangle}{\sqrt{2}}$, autostati di $\boldsymbol{\sigma^1}$ di autovalore ± 1, lo stato di Bell diventa $|\psi^-\rangle = \frac{|-+\rangle - |+-\rangle}{\sqrt{2}}$. Se adesso Alice misura $\boldsymbol{\sigma^1_A}$ ha la probabilità del 50% di ottenere $|+\rangle_A$ o alternativamente $|-\rangle_A$, riuscendo così a dedurre lo stato di Bob in questa nuova base: cambiando la base su cui si effettuano le misure non mutano le proprietà del sistema. Tale fenomeno è peculiare dell'entanglement e porta con sé un'ulteriore conseguenza: se Alice misura su una base può conoscere lo stato di Bob solo in quella specifica base.

Il fatto che Alice possa venire a conoscenza dello stato del sistema di Bob immediatamente a seguito della sua misura, non importa quanto questo sia distante, viola il *principio di località* di Einstein. Esso nella sua formulazione fornita da Bohm può essere così sintetizzato:

Se A e B sono due sistemi tra i quali intercorre una distanza di tipo spazio allora in una teoria completa non è ammissibile che un evento in A modifichi lo stato di B e viceversa.

Per teoria completa si intende una teoria che contenga tutti gli elementi di realtà, ovvero qualunque informazione ottenibile dal sistema indipendentemente dall'esperimento che si effettua. Le conseguenze dell'entanglement, quindi, portarono al cosiddetto *Paradosso EPR* che prende i nome dai fisici che lo formularono: Einstein, Podowsky e Rosen. Essi sostenevano che la meccanica quantistica fosse una teoria incompleta e proposero una teoria detta *delle variabili nascoste*: tale teoria è fondamentalmente una teoria deterministica ma prevede dei gradi di libertà incogniti che suggeriscono un apparente carattere aleatorio.

2.2 Disuguaglianza CSHS

A confutare questa tesi si spese il fisico John Stewart Bell il quale formulò l'omonimo teorema. Esso fissa il limite superiore sui risultati delle misure di determinate osservabili del sistema nell'ipotesi in cui il fenomeno sia regolato da una distribuzione congiunta di probabilità, incarnata appunto dalla variabile nascosta.

Una disuguaglianza molto utilizzata per testare la validità del principio di località, e dunque verificare il teorema di Bell, in meccanica quantistica è la *disuguaglianza CHSH* (John Clauser, Michael Horne, Abner Shimony, Richard Holt) [6]. Per giungere alla disuguaglianza CHSH si consideri un sistema bipartito composto dai sottosistemi A e B. Siano $A(\lambda),\ A'(\lambda),\ B(\lambda),\ B'(\lambda)$, che assumono valori in $[-1, 1]$, degli osservabili rispettivamente di A o di B e λ la variabile nascosta che obbedisce a una certa distribuzione di probabilità $p(\lambda)$.

Ricordando che

$$\langle AB \rangle \stackrel{\text{def}}{=} \int p(\lambda) A(\lambda) B(\lambda) d\lambda, \tag{2.4}$$

possiamo scrivere:

$$\begin{aligned}
&|\langle AB\rangle - \langle AB'\rangle| = |\langle AB(1 \pm A'B')\rangle - \langle AB'(1 \pm A'B)\rangle| \leq 2 \pm (\langle A'B\rangle + \langle A'B'\rangle \\
&|\langle AB\rangle - \langle AB'\rangle| + |\langle A'B\rangle + \langle A'B'\rangle| \leq 2 \\
&|\langle C\rangle| \stackrel{\text{def}}{=} |\langle AB\rangle - \langle AB'\rangle + \langle A'B\rangle + \langle A'B'\rangle| \leq 2
\end{aligned} \tag{2.5}$$

La disuguaglianza CHSH può essere testata sostituendo gli osservabili generici coi seguenti operatori:

$$A \mapsto \boldsymbol{a} \cdot \boldsymbol{\sigma}_A \quad A' \mapsto \boldsymbol{a'} \cdot \boldsymbol{\sigma}_A \quad B \mapsto \boldsymbol{b} \cdot \boldsymbol{\sigma}_B \quad B' \mapsto \boldsymbol{b'} \cdot \boldsymbol{\sigma}_B$$

con

$$|\boldsymbol{a}| = |\boldsymbol{a'}| = |\boldsymbol{b}| = |\boldsymbol{b'}| = 1$$

I versori $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{a'}, \boldsymbol{b'}$ sono separati successivamente di un angolo di $\frac{\pi}{4}$. Se si valuta la grandezza $\langle C \rangle$ sullo stato $|\psi\rangle^{-}_{AB}$ si ottiene

$$|\langle C\rangle| = \left| -4 \cdot \frac{\sqrt{2}}{2} \right| = 2\sqrt{2} \geq 2 \tag{2.6}$$

che è una palese violazione del risultato del teorema di Bell.

2.3 Stati GHZ

Gli *stati GHZ* (Greenberger–Horne–Zeilinger) [10] sono la naturale generalizzazione degli stati massimamente entangled per sistemi costituiti da $M > 2$ sottosistemi. L'esempio più semplice è il caso di 3 Q-bit dove lo stato GHZ può essere

scritto come

$$|GHZ\rangle = \frac{1}{\sqrt{2}}\big(\,|000\rangle + |111\rangle\,\big), \tag{2.7}$$

dove si è usata la notazione compatta $|ijk\rangle = |i\rangle_A \otimes |j\rangle_B \otimes |k\rangle_C$.
Tale stato è contemporaneamente autostato di

$$\boldsymbol{\sigma}^3_A \otimes \boldsymbol{\sigma}^3_B \otimes \boldsymbol{I}_C, \qquad \boldsymbol{I}_A \otimes \boldsymbol{\sigma}^3_B \otimes \boldsymbol{\sigma}^3_C, \qquad \boldsymbol{\sigma}^1_A \otimes \boldsymbol{\sigma}^1_B \otimes \boldsymbol{\sigma}^1_C \tag{2.8}$$

di autovalore 1.
Tali stati possono essere utilizzati per mettere in luce una violazione sistematica, e non statistica, del principio di località di Einstein e dunque si rivelano un utile strumento per distinguere una teoria delle variabili nascoste da una teoria quantistica.
Si considerino i tre sperimentatori Alice, Bob e Charlie ognuno dei quali è in possesso di uno dei Q-bit che insieme costituiscono lo stato $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Ricordando che $i\boldsymbol{\sigma}^2 = \boldsymbol{\sigma}^3\boldsymbol{\sigma}^1$ si vede come $|GHZ\rangle$ è autostato dei seguenti osservabili (a meno di una fase complessa):

$$\boldsymbol{\sigma}^2_A \otimes \boldsymbol{\sigma}^2_B \otimes \boldsymbol{\sigma}^1_C\,|GHZ\rangle = -\,1\,|GHZ\rangle\,; \tag{2.9}$$

$$\boldsymbol{\sigma}^1_A \otimes \boldsymbol{\sigma}^2_B \otimes \boldsymbol{\sigma}^2_C\,|GHZ\rangle = -\,1\,|GHZ\rangle\,; \tag{2.10}$$

$$\boldsymbol{\sigma}^2_A \otimes \boldsymbol{\sigma}^1_B \otimes \boldsymbol{\sigma}^2_C\,|GHZ\rangle = -\,1\,|GHZ\rangle\,. \tag{2.11}$$

Detti s^i_α, con $i \in \{1,2,3\}$ e $\alpha \in \{A,B,C\}$ gli autovalori delle diverse matrici di Pauli, le espressioni precedenti si riassumono in:

$$s^2_A s^2_B s^1_C = s^1_A s^2_B s^2_C = s^2_A s^1_B s^2_C = -1. \tag{2.12}$$

Supponendo il fenomeno regolato da variabili nascoste, ovvero attribuendo carattere predittivo al sistema precedente anche nel caso in cui gli osservatori non effettuino sperimentalmente una specifica misura, si potrebbe inferire il risultato di $\boldsymbol{\sigma}^1_A \otimes \boldsymbol{\sigma}^1_B \otimes \boldsymbol{\sigma}^1_C\,|GHZ\rangle$. Infatti moltiplicando tutte le relazioni si ottiene:

$$(s^2_A s^2_B s^2_C)^2 s^1_A s^1_B s^1_C = -1. \tag{2.13}$$

Essendo $(s^2_A s^2_B s^2_C)^2 > 0$ consegue $s^1_A s^1_B s^1_C = -1$ che è il valore di aspettazione teorico che si otterrebbe se tutti gli sperimentatori misurassero lo stesso osservabile $\boldsymbol{\sigma}^1$. Tuttavia effettuando sperimentalmente l'osservazione risulta

$$\boldsymbol{\sigma}^1_A \otimes \boldsymbol{\sigma}^1_B \otimes \boldsymbol{\sigma}^1_C\,|GHZ\rangle = 1 \tag{2.14}$$

e dunque

$$s^1_A s^1_B s^1_C = 1, \tag{2.15}$$

in aperta contraddizione con la 2.13. Questo prova, ancora una volta, come una teoria delle variabili nascoste non è in grado di riprodurre i risultati della meccanica quantistica.

2.4 Dense Coding

Si supponga di voler inviare un'informazione codificata in un C-bit tramite un canale quantistico, per fare ciò è necessario almeno un Q-bit. Se invece si vogliono codificare 2 C-bit, che vuol dire quattro possibili valori diversi, un unico Q-bit rimane sufficiente a patto di aver precedentemente stabilito tra mittente e destinatario un codice di comunicazione: tale protocollo è definito *Dense Coding* [14]. Per esempio si consideri lo stato entangled $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ e che i due sperimentatori Alice e Bob, distanti tra loro, abbiano precedentemente concordato il seguente *codice*:

$$|\phi^+\rangle \mapsto 00, \tag{2.16}$$
$$|\psi^+\rangle \mapsto 01, \tag{2.17}$$
$$|\phi^-\rangle \mapsto 10, \tag{2.18}$$
$$|\psi^-\rangle \mapsto 11, \tag{2.19}$$

che mappa ognuno dei 4 stati di Bell in uno dei possibili valori che una coppia di bit classici può assumere. È importante sottolineare che il codice è del tutto arbitrario, l'importante è che sia condiviso tra mittente e destinatario senza ambiguità. A questo punto, se Alice ha necessità di trasferire la coppia di C-bit a Bob non deve fare altro che applicare uno tra gli operatori $\boldsymbol{I}$, $\boldsymbol{\sigma}_A^1$, $\boldsymbol{\sigma}_A^2$, $\boldsymbol{\sigma}_A^3$ allo stato entangled inizialmente in suo possesso in modo da mutarlo in uno dei 4 stati di Bell corrispondente, secondo il codice, all'informazione classica che si desidera trasferire e inviarlo a Bob tramite il canale quantistico. A Bob basterà misurare lo stato ricevuto nella base di Bell e, in base all'autodirezione che gli fornisce autovalore 1, risalire alla forma dello stato entangled, quindi tramite il codice dedurre l'informazione classica a esso associata.

2.5 Teletrasporto Quantistico

Si è visto come sia possibile scambiare due C-bit sfruttando un singolo Q-bit, un canale quantistico e un adeguato protocollo. Il processo inverso, ovvero inviare l'informazione racchiusa in un Q-bit tramite un canale classico risulta essere maggiormente ostico. Infatti si consideri il caso in cui si desideri trasmettere uno stato $|\psi\rangle$ tra i due sperimentatori Charlie e Bob utilizzando solo canali classici, ovvero scambiandosi i risultati delle misure senza però poter scambiare lo stato quantistico vero e proprio. Una soluzione potrebbe essere che il mittente, Charlie, misuri $|\psi\rangle$ lungo una generica direzione $\hat{n}$ e invii all'altro il risultato della misura che può essere $|\uparrow_{\hat{n}}\rangle$ o $|\downarrow_{\hat{n}}\rangle$. Una volta ricevuta l'informazione, Bob può costruire uno stato $|\varphi\rangle$ che riproduca con la stessa accuratezza la misura lungo $\hat{n}$ ma è dimostrato che

$F(\psi,\varphi) = |\langle\psi|\varphi\rangle|^2 = \frac{2}{3}$ e che questo è il massimo valore di fedeltà che si può ottenere tramite un qualsiasi protocollo che sfrutti unicamente un canale classico. Tuttavia esiste un protocollo, detto del *teletrasporto* [5], che permette di ottenere il trasferimento dello stato tra Charlie e Bob con fedeltà pari a 1 affiancando all'uso del canale classico l'entanglement tra due stati che gli sperimentatori avevano precedentemente condiviso.

Si considerino 3 Q-bit A, B, C, ognuno in possesso rispettivamente degli sperimentatori Alice, Bob e Charlie e che Alice e Bob condividano le due parti dello stato di Bell $|\phi^+\rangle_{AB} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ mentre Charlie è in possesso dello stato generico $|\psi\rangle_C = a|0\rangle + b|1\rangle$ con $a, b \in \mathbb{C}$. Affinché Bob riesca a risalire con esattezza allo stato di Charlie scambiando con lui solo informazioni classiche è necessario che Charlie si appoggi ad Alice e sfrutti l'entanglement che intercorre tra lo stato di quest'ultima e quello di Bob. Infatti instaurando l'entanglement, questa volta tra C ed A, si ottiene:

$$\begin{aligned}
|\psi\rangle_C |\phi^+\rangle_{AB} &= (a|0\rangle + b|1\rangle)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) \\
&= \frac{1}{\sqrt{2}}\big(a|000\rangle_{CAB} + a|011\rangle_{CAB} + b|100\rangle_{CAB} + b|111\rangle_{CAB} \\
&= \frac{1}{2}a\big(|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA}\big)|0\rangle_B + \frac{1}{2}a\big(|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA}\big)|1\rangle_B + \\
&+ \frac{1}{2}a\big(|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA}\big)|0\rangle_B + +\frac{1}{2}a\big(|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA}\big)|1\rangle_B \\
&= \frac{1}{2}|\phi^+\rangle_{CA}|\psi\rangle_B + \frac{1}{2}|\psi^+\rangle_{CA}\boldsymbol{\sigma}_1|\psi\rangle_B + \\
&+ \frac{1}{2}|\psi^-\rangle_{CA}\big(-i\boldsymbol{\sigma}_2\big)|\psi\rangle_B + \frac{1}{2}|\phi^-\rangle_{CA}\boldsymbol{\sigma}_3|\psi\rangle_B .
\end{aligned} \tag{2.20}$$

A Charlie ed Alice adesso non resta che misurare il loro stato entangled nella base di Bell e inviare il risultato a Bob il quale risulta essere in possesso dello stato $\boldsymbol{\sigma}_i|\psi\rangle_B$ con $i : 0,1,2,3$ e $\boldsymbol{\sigma}_0 \equiv \boldsymbol{I}$, dove $|\psi\rangle$ è esattamente lo stato iniziale di Charlie. Ricevuto il risultato, a Bob basta applicare allo stato in suo possesso l'operatore di Pauli che nella 2.20 è associato allo stato di Bell che Charlie ed Alice gli hanno comunicato; in questo modo, sfruttando la proprietà che $\boldsymbol{\sigma}_i^2 = \boldsymbol{I}$, egli perviene proprio all'informazione che cercava:

$$\boldsymbol{\sigma}_i|\psi\rangle_B \xrightarrow{\text{applica}} \boldsymbol{\sigma}_i\Big[\boldsymbol{\sigma}_i|\psi\rangle_B\Big] = \boldsymbol{\sigma}_i^2|\psi\rangle_B = |\psi\rangle_B . \tag{2.21}$$

Tale processo è perfettamente in accordo con il *teorema no-cloning* [appendice A] infatti, prima di trasferire l'informazione a Bob, la misura effettuata da Alice cancella l'informazione in $|\psi\rangle_C$.

Si possono riassumere i risultati ottenuti in questa sezione e nella precedente introducendo un nuovo tipo di vettore di informazione: l'*E-bit* (entanglement-bit). Esso è utile per schematizzare l'informazione contenuta nell'entanglement dei due stati e come essa venga spesa per trasferire l'informazione, classica o quantistica, nei due protocolli esaminati:

1. *Dense Coding*: 1 E-bit + 1 Q-bit $\longrightarrow$ 2 C-bit;
2. *Teletrasporto*: 1 E-bit + 2 C-bit $\longrightarrow$ 1 Q-bit.

È possibile estendere il protocollo del teletrasporto ad un'informazione contenuta in un numero N di Q-bit [14]. Si consideri dunque uno stato massimamente entangled di due sistemi, A e B, N-dimensionali:

$$|\Phi\rangle_{AB} = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle_A \otimes |i\rangle_B \,, \tag{2.22}$$

il quale gode della proprietà

$$\begin{aligned} {}_{CA}\langle\Phi|\Phi\rangle_{AB} &= \frac{1}{N} \sum_{i,j=0}^{N-1} \big({}_C\langle j| \otimes_A \langle j| \big) \big(|i\rangle_A \otimes |i\rangle_B \big) \\ &= \frac{1}{N} \sum_{i,j=0}^{N-1} |i\rangle_B \, {}_C\langle j| \equiv \frac{1}{N} \mathbf{T}_{BC}. \end{aligned} \tag{2.23}$$

Dove si è introdotto $\mathbf{T}_{BC}$ *operatore di trasferimento* il quale mappa uno stato in C nello stato identico però in B:

$$\mathbf{T}_{BC} |\varphi\rangle_C = \mathbf{T}_{BC} \sum_i a_i |i\rangle_C = \sum_i a_i |i\rangle_B = |\varphi\rangle_B \,. \tag{2.24}$$

Lo stato $|\Phi\rangle$, espresso nella sua decomposizione di Schmidt, diventa

$$|\Phi(\mathbf{U})\rangle_{AB} = \mathbf{U} \otimes \mathbf{I} \, |\Phi\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i'\rangle \otimes |i\rangle = \frac{1}{\sqrt{N}} \sum_{i,j=0}^{N-1} U_{ij} \, |j\rangle_C \otimes |i\rangle_B \,, \tag{2.25}$$

dove

$$\mathbf{U} \, |i\rangle = \sum_j U_{ij} \, |j\rangle = |i'\rangle \,.$$

Si può dimostrare che:

$${}_{CA}\langle\Phi(\mathbf{U})|\Phi(\mathbf{V}^T)\rangle_{AB} = \frac{1}{N} \big(\mathbf{V}\mathbf{U}^{-1} \big)_B \mathbf{T}_{BC}. \tag{2.26}$$

Dunque considerando **U**, un generico operatore unitario, si può scrivere l'operatore di trasferimento come

$$\frac{1}{N}\mathbf{T}_{BC} =_{CA} \langle\Phi(\mathbf{U})|\Phi(\mathbf{U}^T)\rangle_{AB}\,. \tag{2.27}$$

Si supponga, ora, che Charlie si rechi nel laboratorio di Alice per trasferire a Bob lo stato $|\varphi\rangle_C$ perché sa che i due condividono lo stato massimamente entangled $|\Phi\rangle_{AB}$. Alice esegue una misura proiettando lo stato CA e ottiene come risultato $|\Phi(\mathbf{U}_a)\rangle_{CA}$ per una generica matrice unitaria $\mathbf{U}_a$. A questo punto per l'equazione 2.27, Bob sarà in possesso di $|\Phi(\mathbf{U}_a^T)\rangle_{AB}$ e per ottenere l'esatta copia dello stato di Charlie, ricordando che $|\Phi(\mathbf{U}_a^T)\rangle_{AB} = \mathbf{I}_A \otimes \mathbf{U}_a\,|\Phi\rangle_{AB}$, basta che egli applichi al suo stato $\mathbf{U}_a$.

Tale approccio rivela numerosi vantaggi, primo tra tutti la possibilità di generalizzare il discorso a una generica *POVM* [Appendice B] di elementi $\mathbf{M}_a$ purché valga:

$$\mathbf{M}_a^\dagger\mathbf{M}_a \propto |\Phi(\mathbf{U}_a)\rangle\,\langle\Phi(\mathbf{U}_a)|\,. \tag{2.28}$$

Inoltre permette di applicare l'algoritmo anche nel caso in cui inizialmente Alice e Bob condividano lo stato $|\Phi(\mathbf{V}^T)\rangle_{AB}$ anziché $|\Phi\rangle_{AB}$. Infatti per la 2.26 risulta immediato notare che nel momento in cui Alice ottiene $|\Phi(\mathbf{U}_a)\rangle$ come risultato della misura sul suo sistema, Bob risulterà in possesso proprio dello stato $\mathbf{V}\mathbf{U}_a^{-1}\,|\psi\rangle_B$. Dunque gli sarà sufficiente applicare successivamente gli operatori $\mathbf{U}_a\mathbf{V}^{-1}$ per ottenere $|\psi\rangle_B$.

Formalmente lo scopo di tale operazione risulta evidente ma dal punto di vista fisico essa si mostra di più difficile interpretazione. Infatti, esplicitando il significato fisico degli operatori **V** e $\mathbf{U}_a$, appare chiaro che il primo permette di instaurare l'entanglement tra Alice e Bob mentre il secondo riproduce il risultato della misura di Alice sul sistema CA, dunque, temporalmente, l'azione di **V** precede quella di $\mathbf{U}_a$ nonostante la scrittura suggerisca il contrario. La spiegazione va ricercata nel fatto che se inizialmente i due sperimentatori avessero condiviso lo stato $|\Phi(\mathbf{U}_a^T)\rangle_{AB}$, Bob avrebbe ottenuto immediatamente $|\psi\rangle_B$ a seguito della misura di Alice. Nel caso in esame, invece, egli sarà costretto a ruotare nuovamente il proprio stato tramite l'applicazione di $\mathbf{V}^{-1}$ giungendo a $|\Phi\rangle_{AB}$ e solo dopo potrà sfruttare $\mathbf{U}_a$ per ritrovare $|\Phi(\mathbf{U}_a^T)\rangle_{AB}$ e quindi essere in grado di "leggere" lo stato ricercato.
Un'interpretazione parallela può essere la seguente: il Q-bit, dopo che Charlie lo ha preparato nello stato iniziale, procede avanti nel tempo fino alla misura da parte di Alice; a quel punto inverte il suo percorso lungo la linea del tempo procedendo all'indietro verso l'istante in cui era stato instaurato l'entanglement tra Alice e Bob ed infine inverte ancora avanzando nel tempo fino al momento in cui Bob lo riceve nel suo laboratorio. Lungo questo cammino nello spazio-tempo l'azione di

$\mathbf{U}^{-1}$, la misura di Alice, precede la creazione dell'entanglement tramite l'azione di $\mathbf{V}$.

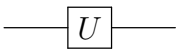
Capitolo 3

Implementazione

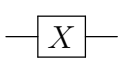
3.1 Quantum Gates

Non tutti i sistemi quantistici possono essere definiti computer quantistici. Il passaggio dall'implementare un singolo Q-bit al costruire una macchina in grado di operare su un array di Q-bit, inizializzabile e sufficientemente isolata dall'ambiente esterno [8] costituisce, ad oggi, uno dei maggiori scogli alla diffusione massiccia di questa nuova tecnologia.

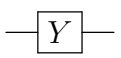
D'altro canto il modello teorico necessario a programmare un computer quantistico è stato sviluppato ed è già ampiamente utilizzato sui computer quantistici esistenti. Esso introduce una nuova notazione secondo la quale i singoli Q-bit sono individuati da linee orizzontali e gli operatori unitari, tramite i quali si opera sui Q-bit, sono schematizzati come porte logiche quantistiche o *quantum gates* [7] [3] che vengono apposte sulle linee corrispondenti ai *quantum registers* Q-bit interessati e nella successione con cui li si intende far agire.



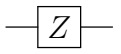
Esempi semplici di gates quantistici sono ovviamente le matrici di Pauli che vengono rappresentate come:



$$\mathbf{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv \boldsymbol{\sigma}_1 \tag{3.1}$$



$$\mathbf{Y} = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \equiv \boldsymbol{\sigma}_2 \tag{3.2}$$



$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \equiv \boldsymbol{\sigma}_3 \tag{3.3}$$

Estremamente utile risulta, senza dubbio, l'*Hadamard Gate*:

$$-\boxed{H}- \quad \mathbf{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(\boldsymbol{\sigma}_1 + \boldsymbol{\sigma}_2). \tag{3.4}$$

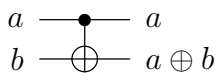
Esso corrisponde a una rotazione di un angolo θ=π lungo la direzione $\hat{n} = \frac{1}{\sqrt{2}}(\hat{n}_1 + \hat{n}_3)$ ovvero a scambiare gli assi $\hat{x}$ e $\hat{z}$, e gode delle seguenti proprietà:

$$\mathbf{H}^2 = \mathbf{I}; \tag{3.5}$$

$$\mathbf{H}\boldsymbol{\sigma}_1\mathbf{H} = \boldsymbol{\sigma}_3; \tag{3.6}$$

$$\mathbf{H}\boldsymbol{\sigma}_3\mathbf{H} = \boldsymbol{\sigma}_1. \tag{3.7}$$

In esse risiede una delle caratteristiche che determinano l'utilità dell'Hadamard ovvero: nelle giuste combinazioni può essere utilizzato per implementare diversi gate. Altro gate di fondamentale importanza è il *controlled-not*:



$$\textbf{CNOT} : |a, b\rangle \rightarrow |a,\ a \oplus b\rangle\,; \tag{3.8}$$

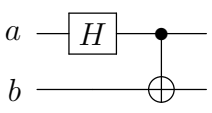
$$\textbf{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \tag{3.9}$$

dove il simbolo $\oplus$ indica la somma modulo 2 e $a, b \in \{0, 1\}$ i quali rappresentano i due Q-bit sui quale agisce il CNOT e prendono rispettivamente il nome di *source* e *target*. Il CNOT è un gate detto *multiline* proprio perché relaziona due Q-bit diversi invertendo o meno il valore del target a seconda che il source sia 1 oppure 0. Esso gode della proprietà:

$$(\textbf{CNOT})^2 = \mathbf{I} \otimes \mathbf{I}. \tag{3.10}$$

Oltre al **CNOT** si possono costruire altri gates quantistici condizionali vincolando l'azione di un certo gate su un generico Q-bit target al valore assunto da un Q-bit source. Un esempio è il **CZ** (*controlled-Z*).

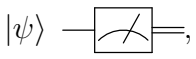
Combinando insieme un Hadamard gate e un CNOT gate è possibile costruire un semplice circuito quantistico in grado di generare uno stato massimamente entangled di due Q-bit. Infatti se il *circuito quantistico* [7]



(3.11)

riceve in ingresso uno degli stati della base $\{|00\rangle, |01\rangle, |10\rangle |11\rangle\}$, lo mappa in uno tra $\{|\phi\rangle^+, |\psi\rangle^+, |\psi\rangle^-, |\phi\rangle^-\}$ stati della base di Bell. In tale circuito si evidenzia la non località dell'azione del CNOT senza la quale, ovviamente, non sarebbe possibile instaurare l'entanglement.

Infine, va menzionato il *measure gate* ovvero il gate che permette di effettuare l'operazione di misura sul Q-bit provocandone il collasso della funzione d'onda e che trasferisce l'informazione ottenuta su un C-bit. I gates preposti ad effettuare operazioni di misura non possono essere schematizzati, dunque, tramite operatori unitari e perciò non sono reversibili:



dove con la doppia linea si indica un canale classico, *classical register*.

3.2 IBM Quantum Experience

Per implementare i protocolli quantistici presentati nelle sezioni 2.4 e 2.5 si è fatto uso dell'*IBM Quantum Experience* [1]. Esso mette a disposizione degli utenti un framework basato sul linguaggio Python (versione 3.7.4) [13] attraverso il quale è possibile sviluppare codice da eseguire su un computer quantistico o un simulatore. In particolare è possibile realizzare il codice tramite la GUI (Graphic User Interface) *Circuit Composer* oppure scrivendo il codice in Python sfruttando la libreria *Qiskit* (versione 0.23.6) [3]. Una volta elaborato il codice desiderato è possibile eseguirlo in Cloud sfruttando il *QASM_Simulator* oppure uno dei computer quantistici che si trovano nei diversi centri di ricerca della IBM.

A seguire saranno presentate le implementazioni degli algoritmi quantistici introdotti nel Capitolo 2 e le differenze che si osservano quando si eseguono su simulatori o su computer quantistici veri e propri.

3.2.1 Dense Coding

Per riuscire a scrivere un codice che esegua il protocollo di Dense Coding sono indispensabili le seguenti librerie (fig. 3.1). In caso in cui non fossero già installate

```
In [1]: #importazione delle librerie
        from qiskit import *
        from qiskit.visualization import plot_histogram
```

Figura 3.1

all'interno del proprio interprete si dovrà scaricare Qiskit [3] e installarla come previsto per il linguaggio Python [13]. Il sorgente in figura 3.2, che sarà analizzato in dettaglio a breve, inizializza il circuito quantistico mostrato in figura 3.3.

In [8]:
```
# Creazione del circuito quantistico.
qc = QuantumCircuit(2)

#STEP 1
# creazione della coppia di Bell tra Alice e Bob.
create_bell_pair(qc, 0, 1)
qc.barrier()

#STEP 2
#Alice e Bob si separano, e lei vuole inviare a lui un messaggio di due C-bit.
#Si è scelto a titolo di esempio il messaggio 10 che viene dunque codificato.
message = "10"
encode_message(qc, 0, message)
qc.barrier()

#Alice invia a Bob il proprio Q-bit.
#Ora Bob è in grado di effettuare misure su entrambi.

#STEP 3
# Bob applica il protocollo di decodifica del messaggio
decode_message(qc, 0, 1)

#STEP 4
#Bob misura entrmbi i Q-bit
qc.measure_all()

# Rappresenzazione del circuito
qc.draw(output = "mpl")
```

Figura 3.2: Codice per l'implementazione del protocollo di Dense Coding

Out[5]:

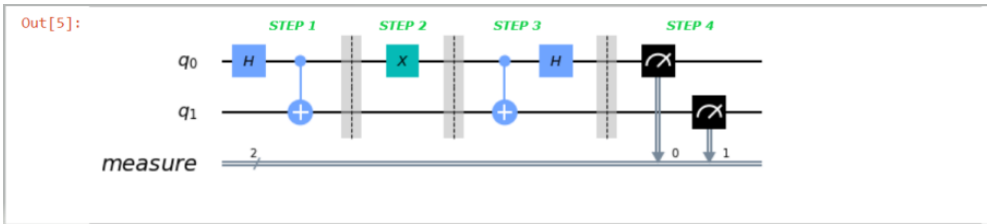


Figura 3.3: Rappresentazione grafica del circuito quantistico preposto al Dense Coding

1. Il primo step del protocollo prevede la preparazione di una coppia di Bell mediante l'apposita funzione *create_bell_pair* (fig. 3.4) la quale prende in ingresso un circuito quantistico e due Q-bit in esso e applica un H-gate sul primo e successivamente un CNOT-gate che ha come source il primo Q-bit e come target il secondo in modo da instaurare l'entanglement tra Bob ed Alice.

In [2]:
```
def create_bell_pair(qc, a, b):
    qc.h(a) #azione di H-gate sul Q-bit a
    qc.cx(a,b) #azione del CNOT-gate tra i Q-bit a e b per instaurare l'entanglement
```

Figura 3.4

2. Per il secondo step si sceglie, senza ledere la generalità, un messaggio di due C-bit che Alice vuole comunicare a Bob -nel caso specifico il messaggio è "10"- e si codifica richiamando la funzione *encode_message* (fig. 3.5). Essa prende in ingresso un registro quantistico, nel protocollo in esame è il Q-bit di Alice, e una stringa che rappresenta il messaggio da codificare.

```
In [3]: def encode_message(qc, qubit, msg):
            if msg == "00":
                pass
            elif msg == "10":
                qc.x(qubit) #azione di X-gate sul Q-bit
            elif msg == "01":
                qc.z(qubit) #azione di Z-gate sul Q-bit
            elif msg == "11":
                qc.z(qubit) #azione di X-gate sul Q-bit
                qc.x(qubit) #azione di X-gate sul Q-bit
                #equivale ad applicare un Y-gate a meno di una fase complessa
            else:
                print("Invalid Message: Sending '00'")
```

Figura 3.5

3. Per il terzo step si suppone che Alice abbia inviato a Bob il proprio Q-bit con il messaggio codificato che ora egli può decodificare tramite la funzione apposita *decode_message* (fig. 3.6). Essa prende in ingresso un circuito quantistico e due Q-bit in esso e applica un CNOT-gate che ha come source il primo Q-bit e come target il secondo, successivamente applica un H-gate sul primo Q-bit.

```
In [4]: def decode_message(qc, a, b):
            qc.cx(a,b) #azione del CNOT-gate tra i Q-bit a e b
            qc.h(a) #azione di H-gate sul Q-bit a
```

Figura 3.6

4. Al quarto e ultimo step Bob esegue una misura su entrambi i Q-bit lungo l'autodirezione $\hat{z}$ ottenendo il valore uno o zero. In base a questa combinazione di valori che risulta dalla misura Bob, è in grado di leggere il messaggio.

Il circuito è stato eseguito in prima istanza sfruttando come backend il simulatore *QASM Simulator* (fig. 3.7) impostando 1024 shots, ovvero ripetendo l'esecuzione 1024 volte e di volta in volta registrando il risultato per poter conseguire consistenza statistica.

```
In [6]: #ESECUZIONE DEL CIRCUITO SUL SIMULATORE
        backend = Aer.get_backend('qasm_simulator')
        job_sim = execute(qc, backend, shots=1024)
        sim_result = job_sim.result()
        #grafico dei risultati
        measurement_result = sim_result.get_counts(qc)
        print(measurement_result)
        plot_histogram(measurement_result)

        {'10': 1024}
```

Figura 3.7

Come è evidente dal risultato della misura riportato nel grafico il simulatore rappresenta un caso ideale, privo del cosiddetto "rumore", e dunque si riesce a risalire al messaggio corretto con accuratezza del 100% (fig. 3.8).

Out[6]:

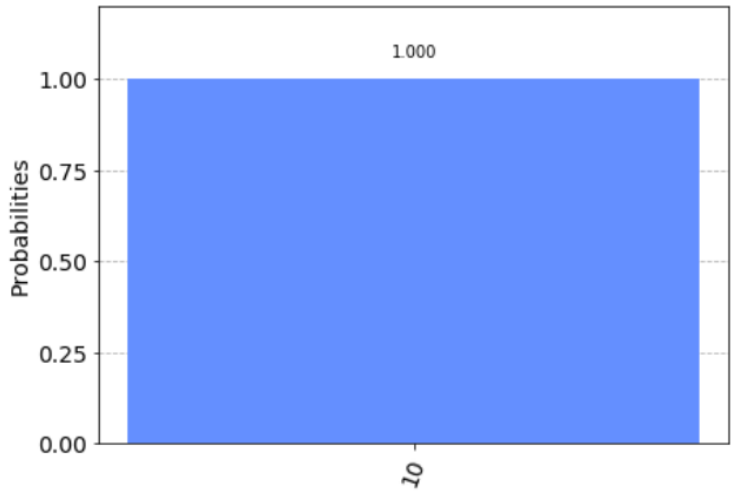


Figura 3.8

Se invece si esegue il circuito su un computer quantistico reale (fig. 3.9), nel caso specifico *ibmq_santiago* (scelto automaticamente a seguito della richiesta di accesso al backend con meno lavori in coda), impostando un numero di shots pari a 256 si ottengono i seguenti risultati.

In [10]:
```
#ESECUZINE DEL CIRCUITO SU UN COMPUTER QUANTISTICO REALE
from qiskit import IBMQ
from qiskit.providers.ibmq import least_busy
shots = 256


IBMQ.load_account()

provider = IBMQ.get_provider(hub='ibm-q')
backend = least_busy(provider.backends(filters=lambda x: x.configuration().n_qubits >= 2
                                       and not x.configuration().simulator
                                       and x.status().operational==True))
print("least busy backend: ", backend)

job = execute(qc, backend=backend, shots=shots)
```

```
Credentials are already in use. The existing account in the session will be replaced.
```

```
least busy backend:  ibmq_santiago
```

Figura 3.9

Dal grafico (fig. 3.10) si evince come nel caso reale il sistema subisca delle interferenze e quindi appare il messaggio corretto con un'accuratezza del 90,23% (fig. 3.11). Impostando una run con 2048 shots, circa dieci volte di più rispetto alla run precedente, si ottiene il risultato in figura. (fig. 3.12, 3.13)

Out[8]:

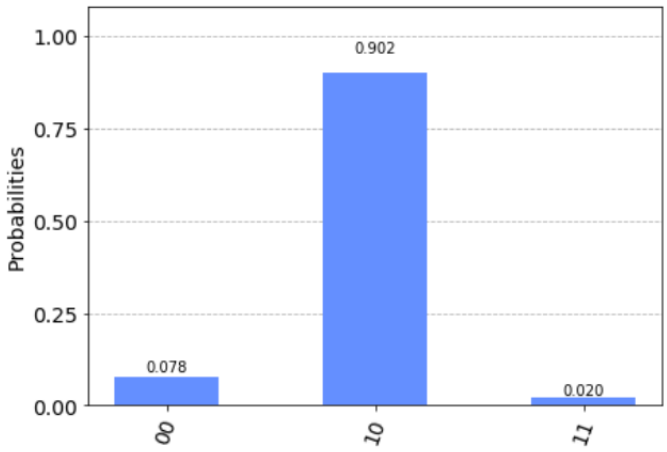


Figura 3.10

In [9]:
```
#valutazione dell'accuratezza percentuale
correct_results = result.get_counts(qc)[message]
accuracy = (correct_results/shots)*100
print("Accuracy = %.2f%%" % accuracy)
```

```
Accuracy = 90.23%
```

Figura 3.11

Out[11]:

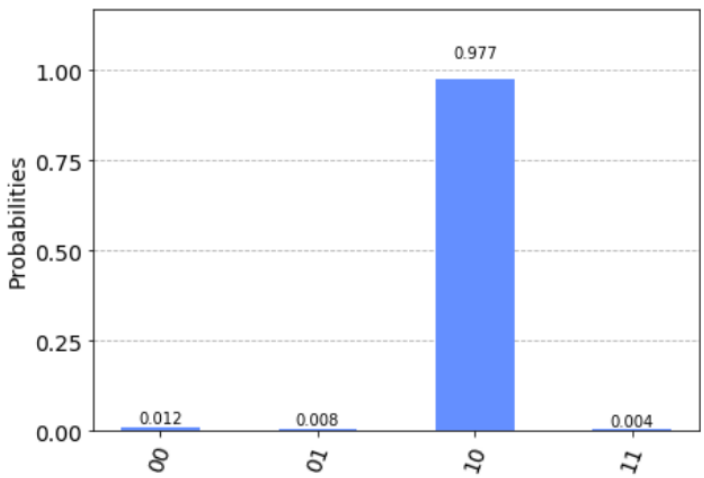


Figura 3.12

In [12]:
```
#valutazione dell'accuratezza percentuale
correct_results = result.get_counts(qc)[message]
accuracy = (correct_results/shots)*100
print("Accuracy = %.2f%%" % accuracy)
```

```
Accuracy = 97.66%
```

Figura 3.13

3.2.2 Teleport

Il sorgente necessario ad implementare il protocollo per il teletrasporto mostra sostanziali differenze a seconda del backend sul quale si intende eseguirlo.
Il sorgente adatto al *QUASM simulator* si presenta in questo modo (fig. 3.14, 3.15):

In [14]:
```
# SETUP
qr = QuantumRegister(3, name = "q" )
crx = ClassicalRegister(1, name = "crx")
crz = ClassicalRegister(1, name = "crz")
cr_result = ClassicalRegister(1, name = "result")
#definizione di un circuito quantistico con gli elementi inizializzati
teleportation_circuit_sim = QuantumCircuit(qr, crx, crz, cr_result)

#STEP 1
#inizializzo in Q-bit di Charlie ad un generico stato psi
teleportation_circuit_sim.append(init_gate, [0])
teleportation_circuit_sim.barrier()

#STEP 2
#creo una coppia di Bell con i Q-bit di Alice e Bob
create_bell_pair(teleportation_circuit_sim, 1, 2)
teleportation_circuit_sim.barrier()

#STEP 3
#crazione dell'entanglement tra la metà dello stato di Bell
#in possesso di Alice e lo stato di Charlie che si vuole trasferire a Bob
alice_gates(teleportation_circuit_sim, 0, 1)

#STEP 4
#Alice e Charlie effettuano una misura dei loro stati
#proiettandoli sulla base di Bell e li inviano figuratamente a Bob
measure_and_send(teleportation_circuit_sim, 1, 0)
teleportation_circuit_sim.barrier()

#STEP 5
#Bob mette in atto il protocollo per ricondurre il proprio stato
#allo stato che inizialmente era in possesso di Charlie
bob_gates(teleportation_circuit_sim, 2, crz, crx)
inverse_init_gate = init_gate.gates_to_uncompute()
#Bob inverte il processso di inizializzazione adottato da Charlie ed effettua la misura
teleportation_circuit_sim.append(inverse_init_gate, [2])
teleportation_circuit_sim.measure(2,2)

#disegno il circuito
teleportation_circuit_sim.draw(output = 'mpl')
```

Figura 3.14

Out[7]:

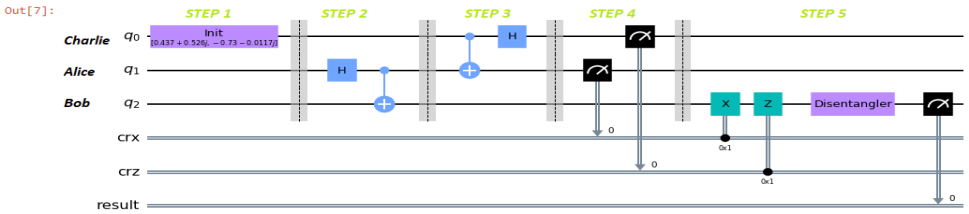


Figura 3.15

Per la sua esecuzione è necessario importare le seguenti librerie (fig. 3.16)

```
In [8]: import numpy as np
        from qiskit import QuantumCircuit, QuantumRegister, ClassicalRegister, execute, BasicAer, IBMQ
        from qiskit.visualization import plot_histogram, plot_bloch_multivector
        from qiskit.extensions import Initialize
        from qiskit_textbook.tools import random_state, array_to_latex
```

Figura 3.16

Il sorgente in figura 3.14 inizia definendo il setup del circuito, il quale necessita di 3 registri quantistici che appartendono rispettivamente a Charlie, Alice e Bob, e altrettanti classici.

1. Nel primo step si inizializza lo stato di Charlie, senza ledere la generalità, ad un generico stato $|\psi\rangle$ tramite il gate *init_gate* così definito mediante le classi *random_state* e *Initialize* (fig. 3.17).

```
In [6]: psi = random_state(1)
        array_to_latex(psi, pretext="|\\psi\\rangle =")
        plot_bloch_multivector(psi)
        init_gate = Initialize(psi)
        init_gate.label = "init"
```

$$|\psi\rangle = \begin{bmatrix} 0.43692 + 0.52557i \\ -0.72989 - 0.01173i \end{bmatrix}$$

Figura 3.17

2. Il secondo step porta alla creazione di uno stato di Bell tra i Q-bit di Alice e Bob mediante l'apposita funzione discussa in 3.2.1.

3. Successivamente Alice instaura l'entanglement con Charlie tramite la funzione *alice_gates* (fig. 3.18).

```
In [3]: def alice_gates(qc, psi, a):
            qc.cx(psi, a) #applica un CNOT-gate tra primo e secondo Q-bit
            qc.h(psi) #applica un H-gate sul primo Q-bit
```

Figura 3.18

4. Al quarto step Alice e Charlie misurano i propri Q-bit lungo l'asse $\hat{z}$ e sfruttano i canali classici *crx* e *crz* per inviare i risultati a Bob.

```
In [4]: def measure_and_send(qc, a, b):
            qc.barrier()
            qc.measure(a,0)
            qc.measure(b,1)
```

5. Infine Bob applica i gate X e Z (figura 3.19) se e soltanto se riceve valore 1 tramite i canali classici crx e crz rispettivamente. Successivamente sfrutta il metotodo *gates_to_uncompute* per definire un gate *disentangler* il quale esegue esattamente l'operazione inversa del gate di inizializzazione. In questo modo il Q-bit di Bob si porterà allo stato 0 se e solo se si trovava precedentemente in uno stato identico a $|\psi\rangle$ a cui era stato inizializzato il Q-bit di Charlie. Per verificare ciò, Bob, infine, procede con la misura del proprio Q-bit.

```
In [5]: def bob_gates(qc, qubit, crz, crx):
            qc.x(qubit).c_if(crx, 1) # Applica X-gate al Q-bit se il crx==1
            qc.z(qubit).c_if(crz, 1) # Applica Z-gate al Q-bit se il crz==1
```

Figura 3.19

Eseguendo il codice e graficando i risultati tramite il comando, si noti come

```
In [15]: backend = BasicAer.get_backend('qasm_simulator')
         counts = execute(teleportation_circuit_sim, backend, shots=1024).result().get_counts()
         plot_histogram(counts)
```

Out[15]:

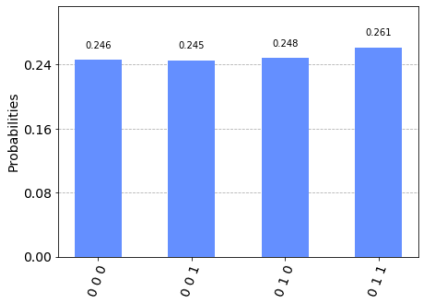


Figura 3.20

ogni terna di possibili risultati abbia come prima cifra il numero 0 (fig. 3.20). Le terne sono costituite dai valori che assumono i tre Q-bit, da destra verso sinistra, alla fine della computazione, perciò, nel 100% dei 1024 shots programmati il Q-bit 2 di Bob si porta allo stato 0. Si può asserire, dunque, il corretto funzionamento del protocollo.

Il protocollo così presentato non è eseguibile su un computer quantistico reale, infatti esso non consente ulteriori manipolazioni su un Q-bit dopo che questi subisce una misura. Tuttavia è possibile applicare il principio della *misura deferenziata* [12] secondo cui le operazioni di misura possono sempre essere spostate da un punto intermedio del circuito alla fine e, nel caso in cui i loro risultati servissero per successive computazioni (proprio come nel caso in esame), è lecito sostituire tutti gli operatori condizionali classici con gli analoghi quantistici.

Perciò è possibile accorpare gli step 4 e 5 in figura 3.14 e scrivere

In [133]:
```
#SETUP
teleportation_circuit_real = QuantumCircuit(3,1)

#STEP 1
#inizializzo in Q-bit di Charlie ad un generico stato psi
teleportation_circuit_real.append(init_gate, [0])
teleportation_circuit_real.barrier()

#STEP 2
#creo una coppia di Bell con i Q-bit di Alice e Bob
create_bell_pair(teleportation_circuit_real, 1, 2)
teleportation_circuit_real.barrier()

#STEP 3
#crazione dell'entanglement tra la metà dello stato di Bell
#in possesso di Alice e lo stato di Charlie che si vuole trasferire a Bob
alice_gates(teleportation_circuit_real, 0, 1)
teleportation_circuit_real.barrier()

#STEP 4-5
#Bob mette in atto il nuovo protocollo per ricondurre il proprio stato
#allo stato che inizialmente era in possesso di Charlie.
new_bob_gates(teleportation_circuit_real, 0, 1, 2)
#Bob inverte il processso di inizializzazione adottato da Charlie ed effettua la misura
inverse_init_gate = init_gate.gates_to_uncompute()
teleportation_circuit_real.append(inverse_init_gate, [2])
teleportation_circuit_real.measure(2,0)

teleportation_circuit_real.draw(output = 'mpl')
```

Out[133]:

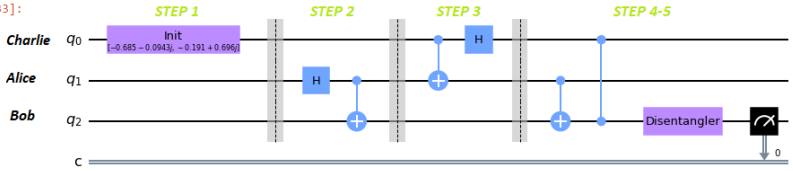


Figura 3.21

dove si è fatto uso della funzione *new_bob_gates* la quale prende in ingresso il circuito quantistico e tutti e tre i Q-bit e applica un CNOT-gate tra il Q-bit di Alice e quello di Bob e un CZ-gate tra quello di Charlie e quello di Bob. Suc-

In [5]:
```
def new_bob_gates(qc, a, b, c):
    qc.cx(b, c) #applica CNOT-gate tra b e c
    qc.cz(a, c) #applica un controlled-Z gate tra a e c
```

Figura 3.22

cessivamente Bob inverte il processo di inizializzazione e procede alla misura, in modo analogo a come descritto nel caso del simulatore.

Impostato il circuito seguendo la stessa procedura del paragrafo 3.2.1 si è provveduto ad inviare il sorgente al backend con minor processi in coda, che è risultato essere nuovamente *ibmq_santiago*, e la sua esecuzione ha prodotto i risultati rappresentati in figura 3.23

In [42]:
```
# selezione del backend con meno lavori in coda
from qiskit.providers.ibmq import least_busy
backend = least_busy(provider.backends(filters=lambda b: b.configuration().n_qubits >= 3 and
                                       not b.configuration().simulator and b.status().operational==True))
print("least busy backend: ", backend)
job_exp = execute(teleportation_circuit_real, backend=backend, shots=8192)
```

```
least busy backend:  ibmq_santiago
```

In [43]:
```
# plotting dei risultati
from qiskit.tools.monitor import job_monitor
job_monitor(job_exp)
exp_result = job_exp.result()
exp_measurement_result = exp_result.get_counts(teleportation_circuit_real)
print(exp_measurement_result)
plot_histogram(exp_measurement_result)
```

```
Job Status: job has successfully run
{'0': 7535, '1': 657}
```

Out[43]:

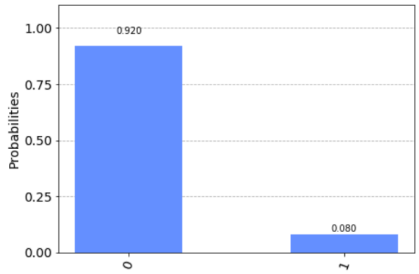


Figura 3.23

Come si può notare, lo stato del Q-bit di Bob non è ritornato al valore zero nella totalità dei casi e ciò è da imputare all'errore casuale dovuto al rumore che affligge le apparecchiature reali. Tuttavia il protocollo è riuscito nella maggioranza dei casi e l'errore risulta, nello specifico, inferiore al 10%:

In [45]:
```
#calcolo dell'errore percentuale
error_rate_percent = sum([exp_measurement_result[result] for result in exp_measurement_result.keys() if result[0]=='1']) \
                     * 100./ sum(list(exp_measurement_result.values()))
print("The experimental error rate : ", error_rate_percent, "%")
```

```
The experimental error rate :  8.02001953125 %
```

Figura 3.24

Va sottolineato che il "prezzo da pagare" per eseguire il protocollo su un computer quantistico reale è la mancanza del trasferimento di informazione classica che permette a Bob di stabilire che gate far agire sul proprio Q-bit. Infatti, se si volesse interpretare l'azione degli operatori condizionali quantistici si potrebbe immaginare come se Alice e Charlie inviassero a Bob i propri Q-bit tramite un canale quantistico ed egli, effettuando delle misure direttamente su di essi, dedurrebbe quali operazioni eseguire sul proprio. Tuttavia in questo modo viene snaturato lo scopo del protocollo: se Charlie avesse a disposizione un canale quantistico potrebbe direttamente trasferire il proprio Q-bit a Bob senza la necessità di ricorrere al teletrasporto.

3.3 Analisi degli errori

Come si è evidenziato nella sezione 3.2, al livello di sviluppo tecnologico odierno non è possibile eliminare del tutto gli errori durante le computazioni effettuate sfruttando un computer quantistico reale. È quindi lecito domandarsi quali siano effettivamente le caratteristiche dell'errore che affligge tali macchine.

Nel presente lavoro si è provato a sondare questo aspetto della computazione per quanto riguarda i due protocolli analizzati avendo cura che l'esecuzione avvenisse sempre tramite il backend *ibmq_santiago* in modo da ottenere maggiore consistenza. Si è quindi modificato il sorgente sostituendo il codice in fig. 3.25 all'algoritomo di selezione del backend con meno lavori in coda.

```
In [ ]: provider = IBMQ.get_provider(hub='ibm-q')
        backend = provider.get_backend('ibmq_santiago')
```

Figura 3.25

Per quanto riguarda il protocollo di Dense Coding si è proceduto ad eseguire il circuito 5 volte per alcuni dei valori di shots nel range $[256, 8196]$ tollerato dal metodo *execute*. Si è poi eseguita una media dei valori ottenuti per ognuno dei messaggi codificati (00, 01, 10, 11) fig. 3.26 e graficato l'andamento di tali valori medi riferiti ai diversi messaggi al variare del numero di shots.

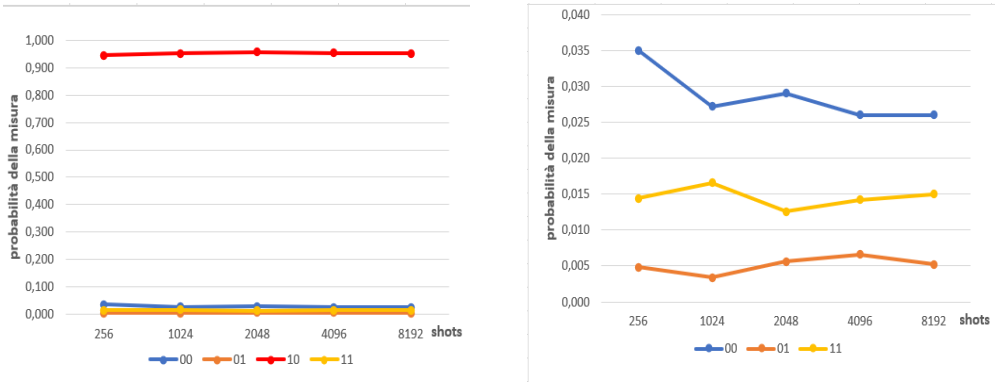
		SHOTS				
		256	1024	2048	4096	8192
MSGs	00	0,035	0,027	0,029	0,026	0,026
	01	0,005	0,003	0,006	0,007	0,005
	10	0,946	0,953	0,957	0,953	0,952
	11	0,014	0,017	0,013	0,014	0,015

Figura 3.26: Valori medi delle misure ottenute per i diversi messaggi codificati nel protocollo di dense coding

Come si vede dal grafico 3.27a e più in dettaglio nel grafico 3.27b l'andamento delle probabilità di occorrenza dei diversi messaggi non risulta particolarmente influenzato dall'incremento di shots. In 3.27b si nota una lieve tendenza a diminuire solo per il messaggio "00" il quale, tuttavia, presenta costantemente occorrenza maggiore rispetto agli altri due messaggi "errati".

Ciò mostra come gli errori non si distribuiscano in maniera uniforme e dunque suggerisce la presenza di un qualche errore sistematico che affligge la macchina.

Replicando la stessa analisi anche per il protocollo del teletrasporto quantistico si sono ottenuti i valori medi riportati in 3.28a e, ancora una volta, il loro



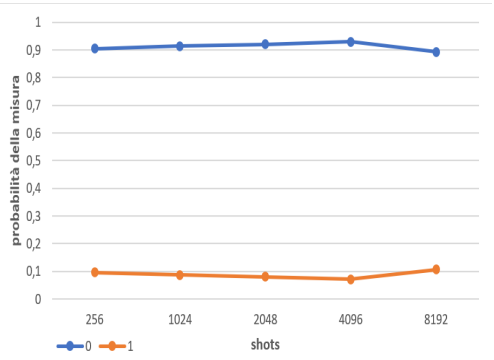
(a) (b)

Figura 3.27: grafici degli andamenti dei valori medi delle misure al variare del numero di shots.

andamento non risulta essere influenzato dal variare del numero di shots 3.28b avvalorando l'ipotesi che il computer *ibmq_santiago* possa essere affetto da errore sistematico.

		SHOTS				
		256	1024	2048	4096	8192
OUTCOME	0	0,904	0,913	0,92	0,929	0,893
	1	0,096	0,087	0,08	0,071	0,107

(a) Tabella



(b) Grafico

Figura 3.28: Andamenti dei valori medi delle misure al variare del numero di shots.

Conclusioni

Dal lavoro svolto si è evidenziato come sia indispensabile saper maneggiare matematicamente i sistemi quantistici aperti per essere in grado di studiare e implementare protocolli efficienti di informazione quantistica.
Si è visto come in tali sistemi si originino fenomeni che cozzano con la descrizione classica che intuitivamente forniamo della realtà; nella fattispecie, tramite la disuguaglianza CHSH e gli stati GHZ, si sono messe in luce violazioni statistiche e sistematiche del principio di località per sistemi bipartiti e tripartiti in cui fosse stato instaurato l'entanglement ed è proprio sull'entanglement che si fondano i protocolli di Dense Coding e Teletrasporto che permettono di superare le difficoltà dettate dal teorema no-cloning nel trasferimento di informazioni.

Nell'implementare i due protocolli mediante l'IBM Quantum Experience ci si è confrontati, contemporaneamente, con le criticità e le potenzialità dei computer quantistici. Infatti le macchine odierne si presentano ancora fortemente imperfette in quanto non si è in grado di isolarle completamente dal rumore ambientale che è sorgente degli errori che sono stati evidenziati. Inoltre, dall'analisi svolta, si è messo in luce anche un carattere sistematico dell'errore che potrebbe essere dovuto sia alle componenti hardware del computer utilizzato, *ibmq_santiago*, che alla componente software del circuito. Parallelamente va chiarito come l'analisi statistica sia stata effettuata su un numero di campioni limitato a causa dei lunghi tempi di esecuzione dei circuiti in cui si incorre quando si rinuncia al protocollo di selezione del backend con meno lavori in coda; quindi potrebbe essere opportuno, in futuro, raccogliere un campione più consistente in modo da consolidare l'evidenza.

Nel perseguire l'obiettivo di ridurre l'errore che affligge le macchine quantistiche una strada sempre più battuta è quella di agire sul software implementando algoritmi di correzione degli errori [11].

Nonostante gli aspetti critici, non possono passare in secondo piano gli imponenti passi avanti che sono stati fatti da quando, negli anni '80 del secolo scorso, si iniziava a ipotizzare lo sviluppo di un computer quantistico fino ad arrivare ad oggi in cui, non solo tali macchine esistono e funzionano in maniera efficiente, ma sono rese disponibili all'intera umanità in cloud tramite l'IBM Quantum Ex-

perience (e altre piattaforme) ma sopratutto si è dimostrata la cosiddetta *quantum supremacy* grazie al processore quantistico a 53 Q-bit, *Sycamore*, di proprietà di Google Inc. [2].

Appendice A

Teorema No-Cloning

Per teorema no-cloning [15] si intende quella peculiare caratteristica della meccanica quantistica la quale vede impossibile creare l'esatta copia di uno stato ignoto senza che questo ne esca modificato. Questo fenomeno risulta di importanza fondamentale nella teoria dell'informazione quantistica perché mentre da un lato apre a nuove strategie crittografiche dall'altro complica notevolmente il trasferimento delle informazioni. L'algoritmo del teletrasporto costituisce proprio una soluzione per superare l'ostacolo del teorema no-cloning nel trasferimento di informazioni.

Il teorema si dimostra per assurdo. Infatti siano dati due stati $|\psi\rangle_A \in \mathcal{H}_A$, incognito, e $|i\rangle_B \in \mathcal{H}_B$ elemento della base ortonormale in B; per ottenere la copia dello stato in A sullo stato in B è necessario ricercare una qualche operazione tale che

$$|\psi\rangle_A \otimes |i\rangle_B \mapsto |\psi\rangle_A \otimes |\psi\rangle_B , \tag{A.1}$$

L'operazione ricercata non può di certo essere un'operazione di misura perché sebbene porterebbe a conoscenza dello stato $|\psi\rangle_A$ e quindi permetterebbe di replicarlo in B, causerebbe il collasso dello stesso nel sistema A cancellandolo definitivamente. Si potrebbe pensare di usare, invece, un operatore di evoluzione temporale $\mathbf{U}(t) = e^{-i\mathbf{H}t/\hbar}$, ovvero di agire sull'hamiltoniana del sistema complessivo in modo da ottenere

$$\mathbf{U}(|\psi\rangle_A \otimes |i\rangle_B) = e^{-i\vartheta(\psi,i)} |\psi\rangle_A |\psi\rangle_B , \tag{A.2}$$

dove ϑ è un generico numero reale che dipende dai due stati. In questo caso si considerino due stati $|\psi\rangle_A$ e $|\varphi\rangle_A$ e, sfruttando l'unitarietà di $\mathbf{U}$ si calcoli:

$$\begin{aligned} \langle\varphi|\psi\rangle \langle i|i\rangle &=_A \langle\varphi|_B \langle i| |\psi\rangle_A |i\rangle_B =_A \langle\varphi|_B \langle i| \mathbf{U}^\dagger\mathbf{U} |\psi\rangle_A |i\rangle_B \\ &= e^{-i(\vartheta(\varphi,i)-\vartheta(\psi,i))}{}_A \langle\varphi|_B \langle\varphi| |\psi\rangle_A |\psi\rangle_B \\ &= e^{-i(\vartheta(\varphi,i)-\vartheta(\psi,i))} \langle\varphi|\psi\rangle^2 , \end{aligned} \tag{A.3}$$

da cui discende banalmente che

$$| \langle \varphi | \psi \rangle |^2 = | \langle \varphi | \psi \rangle | \iff \langle \varphi | \psi \rangle = 0 \ \vee \ \langle \varphi | \psi \rangle = 1 \tag{A.4}$$

contro l'ipotesi di arbitrarietà dei due stati. Quindi si può affermare che non esiste un generico **U**, operatore di evoluzione temporale, che agendo sul sistema completo permetta di copiare lo stato di un sottosistema in un altro sottosistema senza che questo venga modificato.

Appendice B

POVM

Il terzo postulato della meccanica quantistica definisce il formalismo più generale possibile con cui è possibile descrivere l'operazione di misura in meccanica quantistica [12].

POVM è una sigla stante per *positive operative valued measures* e rappresentano un caso particolare delle misure descritte nel postulato. Si consideri uno stato $|\psi\rangle$ e gli operatori di misurazione $\mathbf{M}_m$; la probabilità che la misura produca il risultato *m* sarà data, in accordo col terzo postulato, da:

$$p(m) = \langle\psi|\mathbf{M}^\dagger\mathbf{M}|\psi\rangle\,. \tag{B.1}$$

Se si definisce

$$\mathbf{E}_m = \mathbf{M}^\dagger\mathbf{M},$$

dalle proprietà di $\mathbf{M}$ discende immediatamente che $\mathbf{E}$ è semidefinito positivo e rispetta la relazione di completezza $\sum_m \mathbf{E}_m = \mathbf{I}$ dunque è lecito scrivere:

$$p(m) = \langle\psi|\mathbf{E}_m|\psi\rangle\,. \tag{B.2}$$

Gli elementi $\mathbf{E}_m$ sono detti *elementi POVM* mentre l'insieme $\{\mathbf{E}_m\}$ é la POVM vera e propria ed è sufficiente a determinare le probabilità relative a tutti i possibili risultati della misura.

Le misure proiettive costituiscono un caso particolare delle POVM in cui gli elementi POVM sono i proiettori stessi. Infatti dato il set di proiettori $\mathbf{P}_m$ questi rispettano, per definizione, le relazioni di completezza e ortogonalità

$$\sum_m \mathbf{P}_m = \mathbf{I} \tag{B.3}$$

$$\mathbf{P}_m\mathbf{P}_{m'} = \delta_{mm'}\mathbf{I} \tag{B.4}$$

e quindi è lecito utilizzarli per definire una POVM. Quindi, sempre come conseguenza della definizione di proiettore se si calcolano gli elementi POVM risulta

$$\mathbf{E}_m = \mathbf{P}_m^\dagger \mathbf{P}_m = \mathbf{P}_m. \tag{B.5}$$

Visto come le misure proiettive costituiscano un caso particolare e intuitivo di POVM, ci si potrebbe domandare quali siano le necessità che spingono a introdurre il più generale formalismo POVM piuttosto che limitarsi alle efficaci misure proiettive. Gli argomenti principali sono tre:

- le POVM richiedono che l'operatore rispetti esclusivamente la relazione di completezza mentre le misure proiettive hanno come condizione aggiuntiva la relazione di ortogonalità dei proiettori.

- le misure proiettive hanno insitamente la proprietà di essere ripetibili. Ad esempio, se si misura un generico stato $|\psi\rangle$ e si ottiene

$$|\psi_m\rangle = \frac{\mathbf{P}_m |\psi\rangle}{\sqrt{\langle\psi|\mathbf{P}_m|\psi\rangle}} \tag{B.6}$$

  ripetendo la misura applicando nuovamente $\mathbf{P}_m$ si ha $\langle\psi_m|\mathbf{P}_m|\psi_m\rangle = 1$ ovvero ripetere la misura produce ogni volta lo stesso risultato *m*. Tuttavia questa proprietà matematica risulta incosistente per alcuni sistemi fisici quali potrebbe essere un fotone che viene rivelato da uno schermo. Infatti il fotone al momento della rivelazione viene distrutto e non avrebbe senso parlare di misure successive eseguite su esso.

- Permettono di risolvere il problema di distinguere stati quantistici differenti

Bibliografia

[1] Ibm quantum experience, http://www.research.ibm.com/quantum.

[2] Quantum supremacy using a programmable superconducting processor. *Nature*, 6(574), October 2019.

[3] Abraham Asfaw, Luciano Bello, Yael Ben-Haim, Sergey Bravyi, Nicholas Bronn, Lauren Capelluto, Almudena Carrera Vazquez, Jack Ceroni, Richard Chen, Albert Frisch, Jay Gambetta, Shelly Garion, Leron Gil, Salvador De La Puente Gonzalez, Francis Harkins, Takashi Imamichi, Hwajung Kang, Amir h. Karamlou, David McKay, Antonio Mezzacapo, Zlatko Minev, Ramis Movassagh, Giacomo Nannicni, Paul Nation, Anna Phan, Marco Pistoia, Arthur Rattew, Joachim Schaefer, Javad Shabani, John Smolin, John Stenger, Kristan Temme, Madeleine Tod, Stephen Wood, and James Wootton. Learn quantum computation using qiskit, 2020.

[4] Paul Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *Journal of Statistical Physics*, 22(5):563–591, May 1980.

[5] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, Mar 1993.

[6] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *prl*, 23(15):880–884, October 1969.

[7] Andrew Cross. The IBM Q experience and QISKit open-source quantum computing software. In *APS March Meeting Abstracts*, volume 2018 of *APS Meeting Abstracts*, page L58.003, January 2018.

[8] David P DiVincenzo. Topics in quantum computers. In *Mesoscopic electron transport*, pages 657–677. Springer, 1997.

[9] Richard P. Feynman. Simulating Physics with Computers. *International Journal of Theoretical Physics*, 21(6-7):467–488, June 1982.

[10] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond bell's theorem, 2007.

[11] Robin Harper and Steven T. Flammia. Fault-tolerant logical gates in the ibm quantum experience. *Physical Review Letters*, 122(8), Feb 2019.

[12] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[13] Guido Van Rossum and Fred L. Drake. *Python 3 Reference Manual*. CreateSpace, Scotts Valley, CA, 2009.

[14] R. F. Werner. All teleportation and dense coding schemes. *Journal of Physics A Mathematical General*, 34(35):7081–7094, September 2001.

[15] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *nat*, 299(5886):802–803, October 1982.