Alma Mater Studiorum · Università di Bologna

Scuola di Scienze
Dipartimento di Fisica e Astronomia
Corso di Laurea in Fisica

Quantificare l'entanglement: un protocollo su computer quantistico

Relatore:
Prof.ssa Elisa Ercolessi

Presentata da:
Chiara Cortese

Anno Accademico 2020/2021

Indice

Introduzione

L'entanglement apparve per la prima volta nel panorama della meccanica quantistica nel 1935, in seguito all'articolo «Can Quantum-Mechanical Description of Reality Be Considered Complete» di Einstein, Podolsky e Rosen [9]. Il nome, tuttavia, si deve a Erwin Schrödinger, che utilizzò per primo il termine tedesco *Verschränkung* (lett. intreccio, accavallamento), tradotto poi da lui stesso in "entaglement" [23].
In un ulteriore articolo, «Discussion of Probability Relations between Separated Systems», Schrödinger descrisse l'entanglement [24] così:

> I would not call that *one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.

Cos'è dunque questo fenomeno così importante e centrale nella meccanica quantistica?

L'entanglement è innanzitutto una caratteristica peculiare dei sistemi composti. Preso come esempio un sistema composto da due sottostistemi A e B, lo stato del sistema complessivo AB si dice entangled se non è esprimibile come prodotto tensoriale degli stati dei suoi sottosistemi.
Concretamente, questo implica che esistono particolari correlazioni tra le parti che compongono il sistema tali per cui non è possibile descriverle in modo indipendente l'una dall'altra, così come la perfetta caratterizzazione di ciascuna parte non implica la perfetta conoscenza dello stato complessivo.

Un aspetto molto interessante è che gli stati entangled sono estremamente comuni in natura: basti pensare all'atomo di elio [28], i cui elettroni nello stato di ground hanno i propri spin nello stato $\frac{1}{\sqrt{2}}(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle)$, che fa parte di un set di stati entangled noto come *stati di Bell*. Su tali stati tornerò poi nel corso della trattazione, perché costituiscono un esempio molto importante di stati entangled.

L'entanglement, oltre ad essere un fenomeno quantistico peculiare, è anche una *risorsa*. Esistono infatti alcuni protocolli di comunicazione quantistica, quali il teletrasporto, il dense coding e la crittografia quantistica [28, 1], che si basano proprio sulla realizzazione fisica di stati entangled.

L'entanglement costituisce un'importante risorsa anche nella computazione quantistica. Profilati per la prima volta da Richard Feynman in [10], i computer quantistici sono in grado di offrire, per determinate categorie di algoritmi, un'esponenziale riduzione dei tempi di esecuzione rispetto ai computer classici proprio sfruttando l'entanglement [14].

Il rapporto tra computer quantistico e entanglement è tuttavia molto più profondo. Un computer quantistico reale, proprio per il fatto di essere un dispositivo intrinsecamente legato ai fenomeni quantistici, può essere in grado di effettuare previsioni, riguardo a tali

fenomeni, che non sarebbero mai contemplabili né realizzabili con la semplice computazione classica.
Un esempio di questa enorme potenzialità riguarda la violazione delle disuguaglianze di Bell, che è stata dimostrata anche attraverso esperimenti condotti su computer quantistici reali [8, 16].
Ora, essendo l'entanglement una risorsa e un fenomeno esclusivamente quantistico, appare perfettamente ragionevole guardare ai computer quantistici come dispositivi in grado di portare ad una conoscenza più approfondita di tale fenomeno.

Un tema particolarmente caldo della ricerca sull'entanglement riguarda i possibili modi per quantificarlo. Esiste in letteratura una vasta gamma di misure di entanglement, una cui panoramica è disponibile in [12].
In questa trattazione mi concentrerò su un protocollo che sfrutta le caratteristiche di un computer quantistico per quantificare l'entanglement di una particolare categoria di stati: gli stati misti di rango 2.

Proposto recentemente da A.R. Kuzmak e V.M. Tkachuk in [1], il protocollo si articola in due parti: una prima parte analitica, in cui viene ricavata una formula esatta per il calcolo dell'entanglement, e una seconda parte in cui viene proposta una procedura sperimentale, che prevede la preparazione degli stati su un computer quantistico.

Al fine di poter raggiungere una comprensione profonda del protocollo, ho articolato questo lavoro in 5 capitoli.
Nel primo capitolo viene introdotto il linguaggio degli operatori di densità, indispensabile per trattare gli stati misti, e viene mostrato come i postulati della meccanica quantistica siano riformulabili in tale linguaggio.
Il primo capitolo ospita anche una sezione dedicata ai *qubit*, che sono gli elementi di base della computazione quantistica.

Nel secondo capitolo vengono introdotte alcune nozioni fondamentali della teoria dell'informazione quantistica, tra cui l'entropia di Von Neumann, indispensabile per poter parlare di misura di entanglement.

Il terzo capitolo è interamente dedicato all'entanglement. A partire dalla definizione, vengono riportati e analizzati alcuni esempi di stati entangled (gli stati di Bell) in modo da evidenziare le proprietà di questo particolare fenomeno. Si passa poi al concetto di misura di entanglement, arrivando infine ad introdurre la misura *geometrica* di entanglement, che è quella su cui si basa il protocollo.

Nel quarto capitolo, introdotti ormai tutti gli strumenti necessari, viene presentato e analizzato il protocollo, prestando particolare attenzione a come esso discenda dalla misura geometrica di entanglement e a come sia possile implementarlo a livello sperimentale per un computer quantistico.

Per completare la trattazione, ho applicato il protocollo ad uno stato misto di rango 2 di un sistema a 4 qubit. L'ensemble dello stato misto che ho analizzato è composto soltanto da due stati puri entagled e presenta nella sua composizione una dipendenza parametrica da un numero reale ω. Il ruolo di tale paramentro è valutare come vari l'accuratezza del protocollo sperimentale al variare della composizione dell'ensemble.

Il capitolo quinto ospita tutti i passaggi da me effettuati per tale valutazione e i relativi risultati. Innanzitutto ho ricavato una formula esatta della dipendenza della misura dell'entanglement da ω, realizzata con la parte analitica del protocollo.
Per la parte sperimentale, ho utilizzato la piattaforma IBM Quantum Experience, sviluppata dall'azienda IBM. Tale piattaforma garantisce l'accesso in remoto a computer quantistici reali e loro simulatori.
Dato che per interagire con questi dispositivi occorre impiegare Qiskit, un software development kit sviluppato appositamente dall'IBM, parte del quinto capitolo è dedicata a illustrare le principali funzionalità di tale kit.

Per verificare che il protocollo sperimentale fornisse in un contesto ideale gli stessi risultati del protocollo analitico, ho eseguito una simulazione con `qasm_simulator`, uno dei simulatori disponibili sulla piattaforma.
Infine, ho implementato il protocollo su un dispositivo reale, il computer quantistico `ibmq_santiago`.

Capitolo 1

Il formalismo dell'operatore di densità

La meccanica quantistica fornisce un framework matematico per lo sviluppo delle teorie fisiche. In particolare, i suoi postulati fungono da connessioni tra il mondo fisico e il formalismo matematico che lo andrà a descrivere.
Il loro scopo è definire in che modo venga descritto matematicamente lo stato di un sistema quantistico ad un dato istante, come venga rappresentata la sua evoluzione temporale, come siano descritte e rappresentate le quantità fisiche che lo caratterizzano e come siano descritti i processi di misurazione di tali quantità.
Nella letteratura, i postulati vengono solitamente espressi in termini di vettori di stato, ovvero la descrizione dello stato di un sistema fisico avviene mediante vettori di uno spazio vettoriale complesso, lo spazio di Hilbert.
In teoria dell'informazione quantistica, invece, viene impiegata una formulazione matematicamente equivalente a quella dei vettori di stato ma basata sull'operatore di densità.

In questo capitolo verranno mostrate entrambe le formulazioni sopracitate dei postulati, dopo aver definito il concetto di operatore di densità, e ne verrà mostrata l'equivalenza. Saranno poi presentati i vantaggi della descrizione mediante l'operatore di densità ed alcune sue proprietà fondamentali.

I concetti di seguito esposti fanno riferimento principalmente al capitolo 2 del testo *Quantum Computation and Quantum Information* di M.A. Nielsen & I.L. Chuang [17] e ai capitoli 2 e 3 di *Quantum Mechanics* (Vol.1) di C. Cohen-Tannoudji, B. Diu & F. Laloë [5].

1.1 La notazione di Dirac

Prima di passare ai postulati, è opportuno introdurre la notazione con cui essi verranno enunciati: la notazione di Dirac.

Consideriamo come sistema quantistico una generica particella. Nella notazione di Dirac, ciascuno stato quantistico della particella sarà caratterizzato da un *vettore di stato* appartenente ad uno spazio di Hilbert $\mathscr{E}$, detto *spazio delle fasi* della particella.

Gli elementi dello spazio $\mathscr{E}$ vengono detti vettori *ket* e indicati con la notazione $|\psi\rangle$, dove ψ identifica un arbitrario vettore di $\mathscr{E}$.

Per la presenza di un prodotto scalare interno a $\mathscr{E}$, ad ogni vettore ket $|\psi\rangle \in \mathscr{E}$ è possibile associare un vettore appartenente allo spazio duale di $\mathscr{E}$. Tale vettore è detto vettore *bra* e viene indicato con $\langle\psi|$.
La corrispondenza tra vettore ket e bra è antilineare, ovvero $\lambda_1 |\psi_1\rangle + \lambda_2 |\psi_2\rangle \Longrightarrow \lambda_1^* \langle\psi_1| + \lambda_2^* \langle\psi_2|$, con λ_1, λ_2 costanti complesse e $|\psi_1\rangle$, $|\psi_2\rangle \in \mathscr{E}$.

Riporto di seguito alcune definizioni dell'algebra lineare, in notazione di Dirac, che saranno particolarmente impiegate nei prossimi capitoli.

Definizione 1 (Operatore lineare)**.** Una funzione $A : V \to W$ tra due spazi vettoriali V, W è detta operatore lineare se è lineare nei suoi argomenti, ovvero se

$$A(\sum_i a_i |v_i\rangle) = \sum_i a_i A(|v_i\rangle)$$

con a_i costanti complesse e $|v_i\rangle \in V$.

Definizione 2 (Prodotto interno)**.** Una funzione $(\cdot, \cdot) : V \times V \to \mathbb{C}$ è detta prodotto interno se soddisfa le seguenti condizioni:

(a) $(\cdot, \cdot)$ è lineare nel secondo argomento, ovvero

$$(|v\rangle , \sum_i \lambda_i |w_i\rangle) = \sum_i \lambda_i (|v\rangle , |w_i\rangle)$$

(b) $(|v\rangle , |w\rangle) = (|w\rangle , |v\rangle)^*$

(c) $(|v\rangle , |v\rangle) \geq 0$, con $(|v\rangle , |v\rangle) = 0 \Longleftrightarrow |v\rangle = 0$.

In tal caso si dice che V è dotato di prodotto interno.

Il prodotto interno di due vettori $|v\rangle , |w\rangle \in V$ viene di solito indicato come $\langle v|w\rangle$, dove $\langle v|$ indica appunto il vettore duale di $|v\rangle$, definito come l'operatore lineare da V a valori in $\mathbb{C}$ per cui $\langle v| (|w\rangle) = (|v\rangle , |w\rangle)$, la cui esistenza è garantita dal teorema di Riesz.

Definizione 3 (Prodotto esterno)**.** Siano V, W due spazi vettoriali dotati di prodotto interno. Siano $|v\rangle , |v'\rangle \in V$ e $|w\rangle \in W$. Si definisce prodotto esterno l'operatore lineare $|w\rangle \langle v| : V \to W$ definito da

$$(|w\rangle \langle v|)(|v'\rangle) \equiv |w\rangle \langle v|v'\rangle = \langle v|v'\rangle |w\rangle .$$

Definizione 4 (Autovalori e autovettori)**.** Un autovettore di un operatore lineare A su uno spazio vettoriale V è un vettore non nullo $|v\rangle \in V$ tale che $A|v\rangle = v|v\rangle$, dove v è un numero complesso detto autovalore di A corrispondente a $|v\rangle$.

Definizione 5 (Operatore diagonalizzabile)**.** Un operatore lineare A è detto diagonalizzabile se esiste per esso una rappresentazione $A = \sum_i \lambda_i |i\rangle \langle i|$, dove i vettori $|i\rangle$ formano un set ortonormale completo di autovettori di A, ovvero un set tale per cui $\langle i|j\rangle = \delta_{ij}$, dove δ_{ij} indica la delta di Kronecker, e $\sum_i |i\rangle\langle i| = I$, con I operatore identità.

Definizione 6 (Operatore aggiunto e autoaggiunto)**.** Sia A un operatore lineare su uno spazio di Hilbert V finito dimensionale. Allora esiste unico l'operatore lineare $A^\dagger$, detto operatore aggiunto o hermitiano coniugato, tale che per ogni $|v\rangle , |w\rangle \in V$,

$$(|v\rangle , A|w\rangle) = (A^\dagger |v\rangle , |w\rangle).$$

A è detto operatore autoaggiunto, o hermitiano, se $A^\dagger = A$.

Da questa definizione deriva che per convenzione, dato $|v\rangle$ vettore, si indica $|v\rangle^\dagger \equiv \langle v|$.

Un ulteriore concetto che verrà utilizzato nelle prossime sezioni è la traccia di una matrice. Ogni operatore lineare $A : V \to V$ può essere rappresentato in forma matriciale mediante i coefficienti complessi A_{ij} definiti da $A\,|v_j\rangle = \sum_i A_{ij}\,|v_i\rangle$, con $\{|v_i\rangle\,,\ i = 1, \ldots, n\}$ base ortonormale di V e $|v_j\rangle\,,\ j = 1, \ldots, n$ vettori appartenenti a tale base.
È possibile definire per l'operatore A la funzione *traccia*, definita come $\mathrm{tr}(A) \equiv \sum_i A_{ii}$. Alcune proprietà molto importanti della funzione traccia sono la *ciclicità*, ovvero $\mathrm{tr}(ABC) = \mathrm{tr}(CAB)$, e la linearità. Inoltre, si può dimostrare che la traccia è invariante per trasformazioni unitarie di similitudine $A \to UAU^\dagger$, dato che $\mathrm{tr}(UAU^\dagger) = \mathrm{tr}(UU^\dagger A) = \mathrm{tr}(A)$.

Un'ulteriore utile relazione è (si veda [17] per la dimostrazione)

$$\mathrm{tr}(A\,|\psi\rangle\langle\psi|) = \langle\psi|\,A\,|\psi\rangle\,, \tag{1.1}$$

con $|\psi\rangle$ vettore unitario appartenente al dominio di A.

1.2 I postulati della meccanica quantistica nel formalismo dei vettori di stato

Si riportano di seguito i postulati della teoria della meccanica quantistica nella formulazione dei vettori di stato, assieme ad alcuni esempi e considerazioni.

Postulato 1 (Descrizione dello stato di un sistema)**.** Ad ogni sistema fisico isolato è associato uno spazio vettoriale complesso dotato di prodotto interno, detto *spazio delle fasi* del sistema. Il sistema è completamente descritto dai propri *vettori di stato* $|\psi\rangle$, vettori unitari appartenenti allo spazio delle fasi.
Nel caso di un sistema fisico composto da due o più sottosistemi distinti, lo stato del sistema totale è il prodotto tensoriale degli spazi delle fasi dei sistemi che lo compongono. In particolare, se tali sistemi sono numerati da 1 a n e il sistema i-esimo è preparato nello stato $|\psi_i\rangle$, allora lo stato congiunto del sistema totale è $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$.

Postulato 2 (Descrizione delle quantità fisiche)**.** Ogni quantità fisica misurabile $\mathscr{A}$ di un sistema, detta osservabile, è descritta da un operatore A che agisce nello spazio delle fasi del sistema. Tale operatore è un operatore lineare autoaggiunto.

Il valor medio dell'osservabile $\mathscr{A}$ è legato all'azione di A sul ket di stato $|\psi\rangle$ descrivente il sistema:

$$\langle\mathscr{A}\rangle = \langle\psi|\,A\,|\psi\rangle\,. \tag{1.2}$$

Dalla proprietà di autoaggiunzione discende che l'operatore A avrà autovalori reali a_i e per esso esisterà una base ortonormale di autovettori $|i\rangle$ tali per cui $A = \sum_i |i\rangle\, a_i\, \langle i|$. Questa proprietà è nota come *teorema spettrale*.

Postulato 3 (Evoluzione del sistema)**.** L'evoluzione di un sistema quantistico *chiuso* è descritta da una trasformazione unitaria: lo stato $|\psi\rangle$ di un sistema al tempo t_1 è legato allo stato $|\psi'\rangle$ del sistema al tempo t_2 dalla relazione $|\psi'\rangle = U\,|\psi\rangle$, con U operatore unitario dipendente solo dalla differenza $t_2 - t_1$.

Questo postulato può essere espresso anche in termini di evoluzione continua nel tempo mediante l'*equazione di Schrödinger*:

$$i\hbar\frac{d\left|\psi\right\rangle}{dt} = H\left|\psi\right\rangle,$$

con $\hbar$ costante di Planck ridotta e H Hamiltoniana del sistema. Infatti, essendo H una costante del moto in presenza di sistemi chiusi, è possibile esprimere la soluzione dell'equazione di Schrödinger come:

$$\left|\psi'\right\rangle = \left|\psi(t_2)\right\rangle = \exp\left[\frac{-iH(t_2-t_1)}{\hbar}\right]\left|\psi(t_1)\right\rangle.$$

Postulato 4 (Misurazioni quantistiche)**.** I processi di misurazione sono descritti in meccanica quantistica da una collezione di operatori M_m, detti *operatori di misurazione*, che agiscono sullo spazio delle fasi del sistema oggetto della misurazione. Gli indici m fanno riferimento ai possibili esiti della misurazione. Se il sistema si trova immediatamente prima della misurazione nello stato $\left|\psi\right\rangle$, allora la probabilità che si ottenga l'esito m è

$$p(m) = \left\langle\psi\right| M_m^\dagger M_m \left|\psi\right\rangle, \tag{1.3}$$

e lo stato del sistema dopo la misura sarà

$$\left|\psi'_m\right\rangle = \frac{M_m\left|\psi\right\rangle}{\sqrt{\left\langle\psi\right| M_m^\dagger M_m\left|\psi\right\rangle}}. \tag{1.4}$$

Gli operatori di misura soddisfano l'*equazione di completezza*: $\sum_m M_m^\dagger M_m = I$, con I operatore identità.

L'equazione di completezza garantisce che $\sum_m p(m) = 1$.

1.2.1 Il *quantum bit* come esempio di sistema quantomeccanico

L'esempio più semplice di sistema quantomeccanico è il *quantum bit*, solitamente abbreviato in *qubit*.
I qubit sono sistemi a due stati isolati, ovvero sistemi che possono esistere solo in due stati indipendenti, $\left|0\right\rangle$ o $\left|1\right\rangle$, che sono l'analogo quantistico degli stati 0 e 1 assumibili da un bit classico. Lo stato $\left|0\right\rangle$ è detto stato di ground, mentre lo stato $\left|1\right\rangle$ è detto stato eccitato e insieme formano la cosiddetta *base computazionale*.
Nella pratica, possono essere implementati in generale da sistemi fisici a due stati isolati, ad esempio da fotoni o elettroni. Nel caso dei fotoni, lo stato di ground e lo stato eccitato vengono associati alla polarizzazione orizzontale e verticale della luce. Per gli elettroni invece si considera lo stato di spin: spin $\uparrow$ per lo stato $\left|0\right\rangle$ e spin $\downarrow$ per lo stato $\left|1\right\rangle$.

Lo spazio delle fasi associato al qubit è bidimensionale. Supponendo che i ket $\left|0\right\rangle, \left|1\right\rangle$ formino una base ortonormale per tale spazio, allora un vettore di stato arbitrario potrà essere espresso come $\left|\psi\right\rangle = \alpha\left|0\right\rangle + \beta\left|1\right\rangle$, con α, β numeri complessi tali che $\left|\alpha\right|^2 + \left|\beta\right|^2 = 1$ ($\left|\psi\right\rangle$ deve essere unitario).
Questo esempio mette quindi in luce come il primo postulato implichi anche un *principio di sovrapposizione*, per cui una combinazione lineare di vettori di stato è ancora un vettore di stato.

Nel caso del qubit, gli operatori di misura associati sono due e ad essi sono associati due vettori ortonormali che costituiscono una base per lo spazio delle fasi del qubit.
Sia tale base la base computazionale $\{|0\rangle, |1\rangle\}$. Allora i due operatori di misura possono essere espressi come $M_0 = |0\rangle\langle 0|$ e $M_1 = |1\rangle\langle 1|$. È immediato notare che entrambi gli operatori sono reali e che $M_0^\dagger M_0 = M_0$, $M_1^\dagger M_1 = M_1$ e quindi che $M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1 = |0\rangle\langle 0| + |1\rangle\langle 1|$, che è la rappresentazione in forma di prodotto esterno dell'operatore identità nella base $|0\rangle, |1\rangle$. Gli operatori di misurazione soddisfano quindi l'equazione di completezza.
Supponiamo inoltre che il qubit prima della misura si trovi nello stato $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Allora la probabilità di ottenere l'esito 0 sarà

$$p(0) = \langle\psi| M_0^\dagger M_0 |\psi\rangle = \langle\psi| M_0 |\psi\rangle = \langle \alpha|0\rangle + \beta|1\rangle | \, |\alpha\langle 0|0\rangle|0\rangle + \beta\langle 0|1\rangle|0\rangle\rangle = |\alpha|^2,$$

dove, per ottenere il risultato, si è sfruttata l'ortonormalità della base computazionale.
Analogamente si ha che

$$p(1) = |\beta|^2.$$

I due coefficienti, dunque, devono soddisfare la relazione $|\alpha|^2 + |\beta|^2 = 1$.
Lo stato dopo la misura sarà $\frac{M_0|\psi\rangle}{|\alpha|} = \frac{\alpha|0\rangle}{|\alpha|}$ in caso di esito 0, mentre in caso di esito 1 sarà $\frac{M_1|\psi\rangle}{|\beta|} = \frac{\beta|1\rangle}{|\beta|}$.

I coefficienti complessi α, β sono quindi legati alla probabilità di trovare il qubit, in seguito alla misurazione, nello stato $|0\rangle$ o nello stato $|1\rangle$.

È fondamentale notare come il processo di misurazione comporti il "collasso" del sistema dallo stato di sovrapposizione ad uno dei due stati di base. Se ad esempio l'esito fosse $|0\rangle$, una seconda misurazione produrrebbe ancora $|0\rangle$ con probabilità 1.
L'operazione di misura, dunque, è una trasformazione irreversibile: una volta effettuata, non permette di risalire allo stato iniziale del sistema.

Il processo di misurazione appena descritto è un esempio di una categoria estremamente importante di misurazioni quantistiche: le *misure a valori di proiettore*, solitamente indicate come PVM (dall'inglese *projection-valued measure*).

Definizione 7 (Misura a valori di proiettore)**.** Una PVM è descritta da un operatore di misura M dotato di una decomposizione spettrale

$$M = \sum_m m P_m,$$

dove P_m è il proiettore ortogonale sull'autospazio di M corrispondente all'autovalore m. I possibili esiti della misurazione corrispondono agli autovalori m dell'operatore di misura. In seguito alla misurazione di uno stato $|\psi\rangle$, la probabilità di ottenere l'esito m sarà

$$p(m) = \langle\psi| P_m |\psi\rangle .$$

Se in seguito alla misura si è ottenuto l'esito m, lo stato del sistema sarà

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}.$$

Nelle prossime sezioni, ogni volta che si farà riferimento ad un'operazione di misura, sarà sottinteso che si tratta di una PVM. Questo processo di misura infatti ha la peculiarità

di facilitare il calcolo dei valori medi di aspettazione degli osservabili. Essi infatti si possono esprimere come

$$< m >= \sum_m mp(m) = \sum_m m \langle\psi| P_m |\psi\rangle = \langle\psi| (\sum_m mP_m) |\psi\rangle = \langle\psi| M |\psi\rangle . \tag{1.5}$$

Torniamo allo stato $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. In virtù del fatto che $|\alpha|^2 + |\beta|^2 = 1$, è possibile rappresentare $|\psi\rangle$ come

$$|\psi\rangle = e^{i\gamma}\Big(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\Big), \tag{1.6}$$

con θ, φ, γ numeri complessi.
I termini $e^{i\gamma}$ e $e^{i\varphi}$ sono due termini di fase, detti rispettivamente *fattore di fase globale* e *fase relativa*. Il fattore di fase globale, a differenza della fase relativa, non rappresenta una quantità fisica osservabile. Infatti, se si considerano gli stati $|\Phi\rangle$ e $|\Psi\rangle = e^{i\gamma}|\Phi\rangle$ e un operatore M_m associato ad un qualche processo di misura quantistico, le probabilità di ottenere l'esito m a partire dai due stati sono rispettivamente

$$p(m)_\Phi = \langle\Phi| M_m^\dagger M_m |\Phi\rangle$$
$$p(m)_\Psi = \langle\Psi| M_m^\dagger M_m |\Psi\rangle = \langle\Phi| e^{-i\gamma} M_m^\dagger M_m e^{i\gamma} |\Phi\rangle = e^{-i\gamma+i\gamma} \langle\Phi| M_m^\dagger M_m |\Phi\rangle = p(m)_\Phi.$$

Da un punto di vista osservativo, quindi, gli stati $|\Phi\rangle$ e $|\Psi\rangle$ sono identici. È lecito quindi ignorare il fattore di fase globale nell'Equazione (1.6), che prende quindi la forma

$$|\psi\rangle = \Big(\cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle\Big). \tag{1.7}$$

Questo tipo di rappresentazione è detta *sfera di Bloch*: i numeri complessi θ e φ individuano infatti univocamente i punti di una sfera unitaria, come si può vedere nella Fig.1.1.

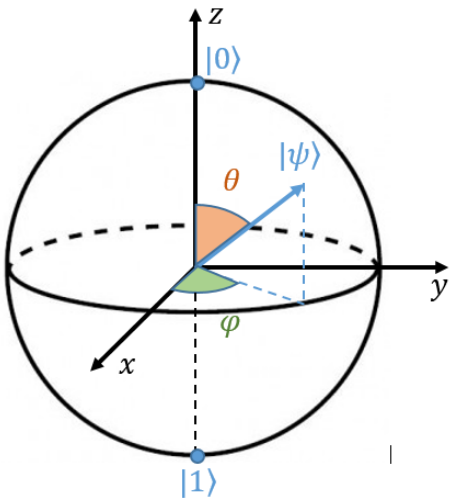


Figura 1.1: Rappresentazione in sfera di Bloch dello stato $|\psi\rangle$ di un qubit.

La sfera di Bloch permette di mettere in corrispondenza 1-1 tutti i possibili stati in cui può trovarsi un qubit con delle terne cartesiane, individuate dagli angoli θ e φ. Gli stati $|0\rangle$ e $|1\rangle$ ad esempio sono individuati rispettivamente da $\theta = 0$ e $\theta = \pi/2$.

La sfera di Bloch è molto utile anche per parlare delle differenze tra l'informazione rappresentata da un bit e quella rappresentata da un qubit.
Immaginiamo che la sfera di Bloch rappresenti un sistema di coordinate geografiche e che un viaggiatore debba comunicare la propria posizione sulla sua superficie. Con un bit classico il viaggiatore sarebbe in grado di dire soltanto se si trova al polo nord (0) o al polo sud (1). Con un qubit, invece, sarebbe in grado di comunicare le coordinate di un punto qualsiasi sulla superficie terreste.
L'informazione infatti nel caso quantistico è racchiusa dai numeri complessi α, β che determinano lo stato del qubit e che a loro volta determinano i valori dei coefficienti θ, ϕ della sfera di Bloch, ovvero le coordinate "geografiche" dell'esempio.

Occorre ricordare però che l'informazione contenuta in un qubit è tale soltanto se il suo stato *non* viene misurato. Se lo si misurasse, si otterrebbe il collasso della sovrapposizione nello stato $|0\rangle$ o nello stato $|1\rangle$, sostanzialmente un bit classico.

1.3 L'operatore di densità

Il formalismo dei vettori di stato si applica molto bene nel momento in cui è possibile determinare perfettamente lo stato iniziale del sistema, ad esempio attraverso un set di misurazioni di valori di osservabili compatibili.[1]
Cosa accade però nel momento in cui si ha a disposizione solo una conoscenza *parziale* dello stato del sistema? Come può essere affrontata nelle previsioni degli esiti di una misurazione questa conoscenza parziale?

Un linguaggio molto conveniente per rispondere a queste domande è costituito dall'operatore di densità.
Supponiamo di avere un sistema quantistico e che tale sistema possa trovarsi in uno degli stati $|\psi_i\rangle$ con probabilità p_i. L'insieme $\{p_i, |\psi_i\rangle\}$ è detto *ensemble di stati puri*.
L'operatore di densità per il sistema rappresentato dall'ensemble è definito dall'equazione

$$\rho \equiv \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right| . \tag{1.8}$$

Si noti che un singolo stato puro è un caso particolare della (1.8) con un solo coefficiente p_i è non nullo.

Vediamo ora come i postulati elencati nella precedente sezione possono essere messi in relazione all'operatore di densità.

Sia U un operatore unitario descrivente l'evoluzione temporale del sistema (che si suppone essere chiuso). Se il sistema si trova inizialmente nello stato $|\psi_i\rangle$ con probabilità p_i allora il sistema si troverà dopo un certo intervallo di tempo nello stato $U|\psi_i\rangle$. L'operatore di densità associato all'evoluzione temporale sarà descritto da

$$\rho \equiv \sum_i p_i \left|\psi_i\right\rangle\!\left\langle\psi_i\right| \xrightarrow{U} \sum_i p_i U \left|\psi_i\right\rangle\!\left\langle\psi_i\right| U^\dagger = U\rho U^\dagger. \tag{1.9}$$

Per quanto riguarda la misurazione, supponiamo di effettuare un processo di misura descritto dall'operatore M_m. Se lo stato iniziale del sistema è $|\psi_i\rangle$ allora la probabilità di

[1] Si intendono gli osservabili corrispondenti ad un set completo di operatori autoaggiunti commutanti.

ottenere l'esito m sarà:

$$p(m|i) = \langle\psi| M_m^\dagger M_m |\psi\rangle = \mathrm{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|), \tag{1.10}$$

dove è stata applicata l'Eq. 1.1.
La probabilità complessiva di ottenere l'esito m sarà dunque

$$p(m) = \sum_i p(m|i)p_i = \sum_i p_i \mathrm{tr}(M_m^\dagger M_m |\psi_i\rangle\langle\psi_i|) = \mathrm{tr}(M_m^\dagger M_m \rho), \tag{1.11}$$

dove sono stati applicati il teorema della probabilità totale, la definizione di operatore di densità e la linearità della funzione traccia.

Andiamo ora a ricavare l'operatore di densità corrispondente al sistema dopo l'operazione di misura.
Dal postulato 4 discende che se lo stato iniziale del sistema è $|\psi_i\rangle$, dopo aver ottenuto il risultato m il sistema si troverà nello stato

$$|\psi_i^m\rangle = \frac{M_m |\psi_i\rangle}{\sqrt{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle}}, \tag{1.12}$$

ovvero dopo la misurazione l'ensemble degli stati sarà $\{p(i|m), |\psi_i^m\rangle\}$.
Applicando il teorema di Bayes, si ha che $p(i|m) = p(m|i)p_i/p_m$ e quindi l'operatore di densità ρ_m risulta, impiegando le eq.1.10 e 1.11:

$$\begin{aligned} \rho_m &= \sum_i p(i|m) |\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m) \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\langle\psi_i| M_m^\dagger M_m |\psi_i\rangle} = \\ &= \sum_i p_i \frac{M_m |\psi_i\rangle\langle\psi_i| M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}. \end{aligned} \tag{1.13}$$

L'operatore di densità è stato introdotto come mezzo per descrivere un ensemble di stati. Al fine di riformulare i postulati della meccanica quantistica, è necessario che l'operatore possa essere caratterizzato in modo indipendente dai vettori di stato. La caratterizzazione della classe di operatori che sono operatori di densità è costituita dal seguente teorema:

Teorema 1 (Caratterizzazione dell'operatore di densità)**.** *Un operatore ρ è l'operatore di densità associato ad un certo ensemble $\{p_i, |\psi_i\rangle\}$ se e solo se soddisfa le seguenti condizioni:*

(a) $tr(\rho) = 1$

(b) ρ *è un operatore positivo, ovvero* $\langle\phi| \rho |\phi\rangle \geq 0$ *per ogni ket di stato arbitrario* $|\phi\rangle$ *.*

Dimostrazione. Supponendo che $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ sia un operatore di densità, sfruttando la relazione 1.1 e la linearità della funzione traccia, si ha che

$$\mathrm{tr}(\rho) = \sum_i p_i \mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i \langle\psi_i| I |\psi_i\rangle = \sum_i p_i \langle\psi_i|\psi_i\rangle = \sum_i p_i = 1,$$

essendo i ket di stato vettori unitari. Per verificare che ρ sia un operatore positivo, considero un vettore di stato arbitrario ϕ nello spazio delle fasi. Allora

$$\langle\phi| \rho |\phi\rangle = \sum_i p_i \langle\phi|\psi_i\rangle \langle\psi_i|\phi\rangle = \sum_i p_i |\langle\phi|\psi_i\rangle|^2 \geq 0 \quad \forall |\phi\rangle .$$

Si consideri un generico operatore ρ positivo e con traccia uguale a 1.
Un operatore positivo è anche necessariamente hermitiano, quindi in virtù del teorema spettrale esisterà per ρ una rappresentazione diagonale:

$$\rho = \sum_k \lambda_k \left|k\right\rangle\!\left\langle k\right|,$$

con λ_k autovalori reali e non negativi di ρ e $|k\rangle$ vettori ortogonali.
Dalla condizione sulla traccia discende che $\sum_k \lambda_k = 1$, perciò ρ corrisponde effettivamente all'operatore di densità dell'ensemble $\{\lambda_k, |k\rangle\}$. □

Attraverso il teorema di caratterizzazione si ottiene dunque una definizione dell'operatore di densità svincolata dal concetto di vettore di stato e che può essere impiegata per riformulare i postulati nel seguente modo.

Postulato 1. Ad ogni sistema fisico isolato è associato uno spazio vettoriale complesso dotato di prodotto interno, detto *spazio delle fasi* del sistema. Il sistema è completamente descritto dal proprio *operatore di densità* ρ, un operatore positivo e con traccia unitaria agente sullo spazio delle fasi. Se un sistema quantistico si trova nello stato ρ_i con probabilità p_i, allora l'operatore di densità del sistema sarà $\sum_i p_i \rho_i$.
Nel caso di un sistema fisico composto da due o più sottosistemi distinti, lo stato del sistema totale è il prodotto tensoriale degli spazi delle fasi dei sistemi che lo compongono. Inoltre, se tali sistemi sono numerati da 1 a n e il sistema i-esimo è preparato nello stato ρ_i, allora lo stato congiunto del sistema totale è $\rho_1 \otimes \rho_2 \otimes \cdots \otimes \rho_n$.

Quest'ultima affermazione deriva dal fatto che, supponendo di avere un operatore ρ_i descrivente un ensemble $\{p_{ij}, |\psi_{ij}\rangle\}$ (i fissato), la probabilità che il sistema si trovi nello stato $|\psi_{ij}\rangle$ sarà $p_i p_{ij}$ e il corrispondente operatore di densità sarà

$$\rho = \sum_{ij} p_i p_{ij} \left|\psi_{ij}\right\rangle\!\left\langle\psi_{ij}\right| = \sum_i p_i \rho_i.$$

Postulato 2. Ogni quantità fisica misurabile $\mathscr{A}$ di un sistema, detta osservabile, è descritta da un operatore A che agisce nello spazio delle fasi del sistema. Tale operatore è un operatore lineare autoaggiunto.

Il secondo postulato rimane invariato, dato che non fa riferimento ai vettori di stato.

Postulato 3. L'evoluzione di un sistema quantistico *chiuso* è descritta da una trasformazione unitaria: lo stato ρ del sistema al tempo t_1 è legato allo stato ρ' del sistema al tempo t_2 dalla relazione $\rho' = U\rho U^\dagger$, con U operatore unitario dipendente solo dagli istanti t_1, t_2.

Postulato 4. I processi di misurazione sono descritti in meccanica quantistica da una collezione di operatori M_m, detti *operatori di misurazione*, che agiscono sullo spazio delle fasi del sistema oggetto della misurazione. Gli indici m fanno riferimento ai possibili esiti della misurazione. Se il sistema si trova immediatamente prima della misurazione nello stato ρ, allora la probabilità che si ottenga l'esito m è

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho), \tag{1.14}$$

e lo stato del sistema dopo la misura sarà

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}. \tag{1.15}$$

Gli operatori di misura devono soddisfano l'*equazione di completezza*: $\sum_m M_m^\dagger M_m = I$.

In questa formulazione, i valori medi associati ad una PVM assumono la forma

$$\langle m \rangle = \mathrm{tr}(M\rho). \tag{1.16}$$

Vediamo ora alcune interessanti proprietà degli operatori di densità.

Innanzitutto, gli operatori di densità consentono di stabilire se un sistema si trova in uno *stato puro* o in uno *stato misto*.
Un sistema quantistico si trova in uno *stato puro* se il suo stato è conosciuto con esattezza, ovvero se può essere rappresentato con un unico vettore $|\psi\rangle$ del suo spazio delle fasi. Il corrispondente operatore di densità sarà semplicemente $\rho = |\psi\rangle\langle\psi|$.
Se ρ non descrive uno stato puro, allora il sistema si troverà in uno *stato misto*.

Nel caso dello stato puro, ρ è un proiettore ortogonale, ovvero un operatore hermitiano idempotente. Infatti, come è stato già detto nella dimostrazione del teorema 1, un operatore positivo è necessariamente anche hermitiano. L'idempotenza si dimostra facilmente applicando ρ ad un vettore di stato arbitrario φ:

$$\rho^2 |\varphi\rangle = (|\psi\rangle\langle\psi|)(\langle\psi|\varphi\rangle |\psi\rangle) = \langle\psi|\varphi\rangle \underbrace{\langle\psi|\psi\rangle}_{=1} |\psi\rangle = \rho |\varphi\rangle .$$

Dall'ultima relazione discende che ρ potrà avere come autovalori soltanto 0 o 1. Dato che $\mathrm{tr}(\rho^2) = \mathrm{tr}(\rho)$ e la traccia di un operatore è pari alla somma dei suoi autovalori, si ha che $\mathrm{tr}(\rho^2) = 1$.

Nel caso più generale dello stato misto, l'operatore di densità sarà nella generica forma $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, dove p_i rappresenta la frazione di elementi dell'ensemble statistico del sistema che si trovano nello stato puro $|\psi_i\rangle\langle\psi_i|$.
Andiamo a ricavare un'espressione per ρ^2:

$$\rho^2 |\varphi\rangle = (\sum_i p_i |\psi_i\rangle\langle\psi_i|)(\sum_i p_i \langle\psi_i|\varphi\rangle |\psi_i\rangle) = \sum_i p_i^2 \langle\psi_i|\varphi\rangle |\psi_i\rangle \Longrightarrow \rho^2 = \sum_i p_i^2 |\psi_i\rangle\langle\psi_i| .$$

La traccia di ρ^2 sarà quindi

$$\mathrm{tr}(\rho^2) = \mathrm{tr}(\sum_i p_i^2 |\psi_i\rangle\langle\psi_i|).$$

Per la linearità della traccia,

$$\mathrm{tr}(\sum_i p_i^2 |\psi_i\rangle\langle\psi_i|) = \sum_i p_i^2 \underbrace{\mathrm{tr}(|\psi_i\rangle\langle\psi_i|)}_{=1} \leq (\sum_i p_i)^2 = 1.$$

Dato che l'uguaglianza è verificata solo per $p_i^2 = p_i = 1$, che corrisponde al caso dello stato puro, la traccia di ρ^2 permetterà di distinguere gli stati puri ($\mathrm{tr}(\rho^2) = 1$) da quelli misti ($\mathrm{tr}(\rho^2) < 1$).

Un'altra caratteristica dell'operatore di densità riguarda la molteplicità di ensemble di stati che è in grado di descrivere. A tal proposito si riporta, senza peraltro dimostrarlo, il seguente teorema:

Teorema 2. *Siano* $\{p_i, |\psi_i\rangle\}$, $\{p_j, |\phi_j\rangle\}$ *due ensemble di stati. I set* $|\tilde{\psi}_i\rangle = \sqrt{p_i}\,|\psi_i\rangle$ *e* $|\tilde{\phi}_j\rangle = \sqrt{p_j}\,|\phi_j\rangle$ *generano lo stesso operatore di densità* $\rho = \sum_i \left|\tilde{\psi}_i\right\rangle\!\left\langle\tilde{\psi}_i\right|$ *se e solo se*

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij} |\tilde{\phi}_j\rangle ,$$

dove u_{ij} è una matrice unitaria a numeri complessi e, nel caso in cui $i \neq j$, il set con il minor numero di elementi viene completato con numero di vettori nulli pari a $|i-j|$.

1.3.1 Rappresentazione in sfera di Bloch per stati misti

La rappresentazione in sfera di Bloch così come è stata introdotta nella scorsa sezione offre una rappresentazione valida solo per gli stati puri.
È possibile estendere tale rappresentazione anche agli stati misti utilizzando il formalismo di Pauli per i sistemi a due stati.
Applicando tale formalismo è possibile infatti esprimere un qualsiasi operatore di densità ρ associato ad uno stato misto come

$$\rho = \frac{I + \vec{r} \cdot \vec{\sigma}}{2}, \tag{1.17}$$

dove I è la matrice identità, $\vec{r}$ un vettore reale a tre componenti di modulo $\|\vec{r}\| \leq 1$ e $\vec{\sigma}$ è un operatore vettoriale le cui componenti in coordinate cartesiane sono le matrici di Pauli:

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1.18}$$

Il vettore $\vec{r}$ è detto *vettore di Bloch* e costituisce la rappresentazione tridimensionale dello stato misto descritto da ρ. L'uguaglianza $\|\vec{r}\| = 1$ si ha nel momento in cui il vettore rappresenta uno stato puro: in tal caso infatti il vettore descrive una sfera unitaria, come da rappresentazione in sfera di Bloch degli stati puri.

I vettori di Bloch sono particolarmente utili per semplificare il calcolo degli autovalori dell'operatore di densità. Tali autovalori infatti sono espressi dalla relazione

$$\lambda_{1,2} = \frac{1}{2}(1 \pm \|\vec{r}\|).$$

Dimostrazione. Sia $\vec{r} = (r_1, r_2, r_3)$. Allora ρ risulta

$$\rho = \frac{1}{2} \begin{pmatrix} 1 + r_3 & r_1 - ir_2 \\ r_1 - ir_2 & 1 - r_3 \end{pmatrix}$$

Procedendo al calcolo degli autovalori:

$$\det[\rho - \lambda I] = 0 \implies \det \begin{pmatrix} 1 + r_3 - 2\lambda & r_1 - ir_2 \\ r_1 - ir_2 & 1 - r_3 - 2\lambda \end{pmatrix} = 0 \implies (1-2\lambda)^2 - r_3^2 - r_1^2 - r_2^2 = 0$$

da cui si ottiene, come volevasi dimostrare, che

$$\lambda_{1,2} = \frac{1}{2}(1 \pm \|\vec{r}\|).$$

□

1.3.2 La descrizione dei sistemi composti: l'operatore di densità ridotto e la traccia parziale

Una delle maggiori applicazioni dell'operatore di densità riguarda la descrizione dei sottosistemi di sistemi composti.
In particolare, prendiamo un sistema quantistico formato da due sottosistemi A e B. Se

si vogliono effettuare delle misurazioni dei valori un'osservabile di A, al fine di ottenere delle previsioni corrette occorrerà prendere in considerazione non l'operatore di densità ρ^{AB} del sistema totale, bensì l'*operatore di densità ridotto* per il sistema A, definito come

$$\rho^A \equiv \mathrm{tr}_B(\rho^{AB}), \tag{1.19}$$

dove tr_B è la *traccia parziale* sul sistema B, definita dall'equazione

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \,\mathrm{tr}(|b_1\rangle\langle b_2|) = |a_1\rangle\langle a_2| \,\langle b_1|b_2\rangle\,, \tag{1.20}$$

con $|a_1\rangle\,,\ |a_2\rangle$ vettori arbitrari dello spazio delle fasi di A e $|b_1\rangle\,,\ |b_2\rangle$ vettori arbitrari dello spazio delle fasi di B.
Perché occorre utilizzare proprio la funzione di traccia parziale? Immaginiamo di voler misurare il valore di un osservabile di A il cui operatore di misura associato è M. Indichiamo poi con $\tilde{M}$ il corrispondente operatore di misura per il sistema AB.
Ora, se AB viene preparato nello stato $|m\rangle\,|\psi\rangle$, con $|m\rangle$ autostato di M con autovalore m e $|\psi\rangle$ generico stato di B, allora l'esito della misurazione dovrà necessariamente essere m con probabilità $p_m = 1$. Di conseguenza, $\tilde{M}$ dovrà assumere la forma $M \otimes I_B$, dove I_B rappresenta l'operatore identità per il sistema B.
Supponiamo ora di voler associare ad A un operatore di densità ρ^A. Per questioni di coerenza fisica, necessariamente i valori medi dell'osservabile calcolati su ρ_A dovranno essere gli stessi calcolati sull'operatore di densità ρ^{AB} del sistema composto. Questo impone che $\mathrm{tr}(M\rho^A) = \mathrm{tr}(\tilde{M}\rho^{AB}) = \mathrm{tr}((M \otimes I_B)\rho^{AB})$, equazione sempre soddisfatta se si sceglie $\rho^A \equiv \mathrm{tr}_B(\rho^{AB})$.[2]

Molte delle proprietà dei sottostistemi di sistemi composti sono determinate dagli autovalori dei propri operatori di densità ridotti.
Nel caso di sistemi composti in uno stato puro, gli operatori di densità ridotti avranno gli stessi autovalori. Questo importante risultato discende dalla decomposizione di Schmidt, un teorema fondamentale per lo studio dei sistemi composti.

Teorema 3 (Decomposizione di Schmidt)**.** *Sia $|\psi\rangle$ uno stato puro di un sistema composto AB. Allora esistono una base di stati ortonormali $|i_A\rangle$ per il sistema A e una base di stati ortonormali $|i_B\rangle$ per B, dette* basi di Schmidt*, tali per cui*

$$|\psi\rangle = \sum_i \lambda_i \,|i_A\rangle\,|i_B\rangle\,,$$

con λ_i numeri reali non negativi soddifacenti la relazione $\sum_i \lambda_i^2 = 1$, detti coefficienti di Schmidt.

Nel caso di uno stato puro, quindi, gli operatori di densità ridotti del sistema AB risultano essere $\rho^A = \sum_i \lambda_i^2 \,|i_A\rangle\langle i_A|$ e $\rho^B = \sum_i \lambda_i^2 \,|i_B\rangle\langle i_B|$ e pertanto hanno gli stessi autovalori λ_i^2.

Vediamo alcune proprietà dei coefficienti di Schmidt che saranno utili più avanti.
Innanzitutto, i coefficienti sono invarianti per trasformazioni unitarie su A e B. Infatti, se considero l'azione di U operatore unitario su A, ottengo che la decomposizione di Schmidt di $U\,|\psi\rangle$ sarà $U\,|\psi\rangle = \sum_i \lambda_i (U\,|i_A\rangle)\,|i_B\rangle$.
Inoltre, verrà mostrato nella prossima sezione che i coefficienti di Schmidt possono quantificare l'entanglement tra due sottostistemi.

[2] È possibile dimostrare che la traccia parziale è l'unica funzione dotata di questa proprietà (cfr. p.107 del testo di Nielsen & Chuang [17]).

Appare chiaro il vantaggio di poter effettuare una decomposizione di Schmidt sullo stato di un sistema, per quanto sia applicabile ai soli stati puri.
È possible estendere questi vantaggi anche agli stati misti grazie alla *purificazione*.
Si tratta di una procedura matematica che permette di associare ad ogni stato misto uno stato puro mediante l'introduzione di un altro sistema, detto *sistema di riferimento*.

Teorema 4. *Sia ρ^A l'operatore associato allo stato di un sistema A. È possibile introdurre un ulteriore sistema R e definire per il sistema complessivo AR uno stato puro $|AR\rangle$ tale per cui $\rho^A = tr_R(|AR\rangle\langle AR|)$.*

Dimostrazione. Suppongo che ρ^A abbia una decomposizione ortonormale $\sum_i p_i \, |i_A\rangle\langle i_A|$.
Introduco un sistema R con associato lo stesso spazio delle fasi di A e dotato di una base ortonormale $|i_R\rangle$.
A questo punto, si può definire lo stato puro $|AR\rangle$ come

$$|AR\rangle \equiv \sum_i \sqrt{p_i} \, |i_A\rangle \, |i_R\rangle \, .$$

Andando a calcolare l'operatore di densità ridotto per il sistema A, si ottiene che

$$\mathrm{tr}_R(|AR\rangle\langle AR|) = \sum_{ij} \sqrt{p_i p_j} \, |i_A\rangle\langle j_A| \, \mathrm{tr}(|i_R\rangle\langle j_R|) = \sum_{ij} \sqrt{p_i p_j} \, |i_A\rangle\langle j_A| \, \delta_{ij} = \sum_i p_i \, |i_A\rangle\langle i_A| \, ,$$

che corrisponde alla definizione di ρ^A. □

Capitolo 2

Teoria dell'informazione quantistica: alcune nozioni di base

Prima di passare all'argomento centrale di questa trattazione, l'entanglement, è fondamentale porre l'attenzione su come viene trattata l'informazione in fisica quantistica e in particolare in che cosa tale trattazione di distingue dalla propria controparte classica.
Alcune nozioni, prima fra tutte l'entropia di Von Neumann, ricoprono infatti un ruolo importante nel quantificare l'entanglement.

In questa sezione verranno presentati, attraverso il confronto con le loro controparti classiche, i concetti di entropia quantistica e di informazione accessibile. Il tutto sarà preceduto da una sezione dedicata ai sistemi a più qubit e alle trasformazioni ad essi applicabili, a completamento di quanto detto riguardo ai qubit nel precedente capitolo.

I testi di riferimento per le sezioni di questo capitolo sono *Quantum Computing. A Gentle Introduction* [22], capitoli 2, 3 e 5 per la sezione 2.1, il capitolo 5 delle *Lecture Notes for Ph219/CS219: Quantum Information and Computation* [20] per le sezioni 2.2 e 2.3.

2.1 Sistemi a più qubit

Nella sezione 1.2.1 è stato presentato il qubit come semplice esempio di sistema quantomeccanico. Esso tuttavia è fondamentale per due motivi: è relativamente semplice da trattare a livello analitico grazie al formalismo di Pauli per i sistemi a due stati ed è il tassello centrale della teoria dell'informazione quantistica.
Il qubit infatti rappresenta l'unità fondamentale dell'informazione quantistica.

Si consideri un sistema a n qubit. Dal Postulato 1 discende che lo spazio delle fasi associato a tale sistema è il prodotto tensoriale degli spazi delle fasi dei singoli qubit che lo compongono.
Lo stato del sistema sarà rappresentabile dunque come segue. Sia V_i con base $\{|0\rangle_i, |1\rangle_i\}$, $0 \leq i < n$, lo spazio vettoriale bidimensionali associato all'i-esimo qubit.
Lo spazio delle fasi del sistema complessivo sarà dato da $V_0 \otimes V_1 \otimes \cdots \otimes V_{n-1}$, che è uno spazio di Hilbert con dimensione 2^n. La base standard[1] per tale spazio sarà composta dai

[1]Con base standard si intende il caso in cui la base computazionale sia formata da da $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

seguenti 2^n vettori:

$$\begin{aligned}\{ &|0\rangle_0 \otimes |0\rangle_1 \otimes \cdots \otimes |0\rangle_{n-1}\,, \\ &|0\rangle_0 \otimes |0\rangle_1 \otimes \cdots \otimes |1\rangle_{n-1}\,, \\ &|0\rangle_0 \otimes |1\rangle_1 \otimes \cdots \otimes |0\rangle_{n-1}\,, \\ &\dots\,, \\ &|1\rangle_0 \otimes |1\rangle_1 \otimes \cdots \otimes |1\rangle_{n-1}\}\end{aligned}$$

Per indicare questi ket di base viene utilizzata solitamente una notazione più compatta, in cui si sottintende il prodotto tensoriale[2]: $\{|0\dots00\rangle\,, |0\dots01\rangle\,, |0\dots10\rangle\,, \dots\,, |1\dots11\rangle\}$. In questa notazione, ciascun ket è identificato essenzialmente da un numero in codice binario, perciò si può ottenere una forma ancora più compatta associando a ciascuno di essi il corrispondente numero decimale[3].
Si consideri a titolo di esempio un sistema formato da due qubit. La base computazionale associata al sistema sarà $\{|00\rangle\,, |01\rangle\,, |10\rangle\,, |11\rangle\}$, esprimibile anche come $\{|0\rangle\,, |1\rangle\,, |2\rangle\,, |3\rangle\}$. Analogamente al caso del singolo qubit, il sistema potrà trovarsi anche in una sovrapposizione degli stati di base, descritta dalla combinazione lineare di ket

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle = \sum_{j=0}^{3} \alpha_j\,|j\rangle\,,$$

con α_0, α_1, α_2, α_3 numeri complessi detti *ampiezze*. Il modulo quadro di ciascun coefficiente rappresenta la probabilità di trovare il sistema, in seguito ad una misurazione, rispettivamente nella configurazione 00, 01, 10 o 11.
I coefficienti dovranno quindi soddisfare la relazione $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$.
Lo stato di un sistema a 2 qubit, dunque, è univocamente determinato da un set di 4 numeri complessi.

Generalizzando al caso di un sistema a n qubit, si ha che ogni stato del sistema è esprimibile mediante la combinazione

$$|\Psi\rangle = \sum_{j=0}^{2^n-1} \alpha_j\,|j\rangle\,,$$

determinato da 2^n coefficienti complessi.

2.1.1 Interagire con i qubit: le trasformazioni unitarie

Nelle precedenti sottosezioni sono state elencate alcune delle proprietà fondamentali dei qubit. Per poter parlare di informazione quantistica e di computazione quantistica è tuttavia necessario un ulteriore tassello: come "interagire" con i qubit, ovvero come si possano realizzare manipolazioni dello stato di uno o più qubit.

La rappresentazione sulla sfera di Bloch sarà particolarmente utile per visualizzare le operazioni di manipolazione. Ad esempio, il passaggio dallo stato $|0\rangle$ allo stato di sovrapposizione $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, solitamente indicato con $|+\rangle$, è descrivibile come una rotazione di

[2] Viene spesso utilizzata anche la notazione $|0\rangle_0 \otimes |0\rangle_1 \otimes \cdots \otimes |0\rangle_{n-1} = |0\rangle\,|0\rangle \dots |0\rangle\,$, $|0\rangle_0 \otimes |0\rangle_1 \otimes \cdots \otimes |1\rangle_{n-1} = |0\rangle\,|0\rangle \dots |1\rangle$, etc.

[3] La notazione decimale può essere ambigua: anche nel caso di un sistema a tre qubit vi sono gli stati di base $|0\rangle\,, |1\rangle\,, |2\rangle\,, |3\rangle$, ma identificano i vettori $|000\rangle\,, |001\rangle\,, |010\rangle\,, |011\rangle$. Occorre quindi precisare di volta in volta il numero di qubit che si stanno considerando.

$\pi/2$ del vettore $|0\rangle$ attorno all'asse y della sfera di Bloch.

Come per la computazione classica, anche in computazione quantistica operazioni di complessità arbitraria possono essere realizzate come composizioni di trasformazioni più semplici. In particolare, qualsiasi trasformazione di stato su un sistema a n qubit può essere realizzata con una sequenza di trasformazioni agenti contemporaneamente solo su 1 o 2 qubit del sistema, che prendono il nome di *quantum gate*. Tali sequenze di gate quantistici sono dette *circuiti quantistici*.
Da un punto di vista pratico, sarebbe auspicabile l'esistenza di un set *finito* di gate quantistici in grado di generare trasformazioni arbitrarie. In realtà, ciò non è possibile in forma esatta: esistono soltanto dei set finiti di gate in grado di riprodurre in forma approssimata tali trasformazioni arbitarie, seppure con arbitraria precisione. Quest'ultimo risultato discende dal teorema di Solovay-Kitaev[4].

Non tutte le trasformazioni possono essere applicate allo stato di un qubit: per effetto del Postulato 3, l'evoluzione temporale di un sistema quantistico isolato deve essere descritta da una trasformazione unitaria U. Un'importante conseguenza dell'unitarietà è che le trasformazioni effettuate sui qubit saranno *invertibili*. Da questa proprietà discende che gli operatori di misura *non* costituiscono dei gate quantistici, dato che la loro azione non è reversibile.

Le radici del postulato sopracitato risiedono nel fatto che le trasformazioni sugli stati di un sistema isolato devono garantire sia che una sovrapposizione di stati venga mandata nella sovrapposizione delle loro immagini, sia che venga preservato dalla trasformazione il modulo unitario dei vettori. Infatti, se i vettori trasformati non fossero unitari, ad essi non sarebbe associato alcuno stato del sistema quantistico, il che è chiaramente un assurdo.

Una conseguenza molto importante della condizione di unitarietà è il *teorema di non-clonazione quantistica*.
Supponiamo che esista una trasformazione unitaria U clonante, ovvero tale che $U(|a\rangle\,|0\rangle) = |a\rangle\,|a\rangle$ per ogni stato $|a\rangle$ di un sistema quantistico. Sia $|c\rangle = \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$ una sovrapposizione di due stati ortogonali $|a\rangle, |b\rangle$ non noti a priori. Per la linearità di U,

$$U(|c\rangle\,|0\rangle) = \frac{1}{\sqrt{2}}(U(|a\rangle\,|0\rangle) + U(|b\rangle\,|0\rangle)) = \frac{1}{\sqrt{2}}(|a\rangle\,|a\rangle + |b\rangle\,|b\rangle).$$

Tuttavia U è una clonazione, perciò

$$U(|c\rangle\,|0\rangle) = |c\rangle\,|c\rangle = \frac{1}{2}(|a\rangle\,|a\rangle + |a\rangle\,|b\rangle + |b\rangle\,|a\rangle + |b\rangle\,|b\rangle),$$

che non corrisponde a quanto ottenuto applicando la proprietà di linearità. Di conseguenza, non esiste una trasformazione unitaria in grado di clonare esattamente un *qualsiasi* stato quantistico di un sistema.
Il teorema di non-clonazione, tuttavia, non nega del tutto la possibilità di duplicare uno stato: se lo stato da clonare appartiene ad un set ortogonale di stati conosciuto a priori, allora la duplicazione avviene senza errori.

Vediamo ora alcune delle trasformazioni che verranno poi utilizzate nelle prossime sezioni.

[4]All'enunciato di questo teorema è dedicata l'Appendice 3 del testo *Quantum Computation and Quantum Information*[17].

Le trasformazioni di Pauli

Le *trasformazioni di Pauli* sono le trasformazioni su singolo qubit più utilizzate. Sono qui riportate sia in forma matriciale sia in decomposizione spettrale:

$$
\begin{aligned}
I &: |0\rangle\langle 0| + |1\rangle\langle 1| \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
X &: |1\rangle\langle 0| + |0\rangle\langle 1| \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
Y &: |0\rangle\langle 1| - |1\rangle\langle 0| \quad \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \\
Z &: |0\rangle\langle 0| - |1\rangle\langle 1| \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}
$$

I è la matrice identità, X è l'equivalente dell'operazione logica classica di negazione (manda $|0\rangle$ in $|1\rangle$ e viceversa) e Z rappresenta una variazione della fase relativa di una sovrapposizione nella base standard. Y invece corrisponde a ZX, ovvero ad una combinazione di negazione e variazione di fase relativa. In letteratura viene spesso considerata come trasformazione Y l'operatore $-i(|0\rangle\langle 1| - |1\rangle\langle 0|)$ anziché $|0\rangle\langle 1| - |1\rangle\langle 0|$, perché così facendo si ottiene una trasformazione Y Hermitiana, che è una proprietà utile nel momento in cui si considerano anche operazioni di misurazione.

La matrici di Pauli godono di due interessanti proprietà:

(a) dal momento che descrivono rotazioni attorno agli assi cartesiani della sfera di Bloch, sono in grado di generare tutte le rotazioni possibili sulla sfera di Bloch e quindi costituiscono una base per qualunque trasformazione a singolo qubit;

(b) $X^2 = -Y^2 = Z^2 = I$.

In Fig.2.1 sono mostrati i simboli circuitali associati alle trasformazioni di Pauli X, Y e Z.

Figura 2.1: Simboli circuitali dei gate associati alle trasformazioni di Pauli: X-gate, Y-gate e Z-gate.

L'Hadamard gate

Un'altra importante trasformazione a un qubit è la *trasformazione di Hadamard*:

$$
H : \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 1|) \quad \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}
$$

Questa trasformazione viene spesso indicata anche come

$$
\begin{aligned}
H : |0\rangle \rightarrow |+\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\
|1\rangle \rightarrow |-\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)
\end{aligned}
$$

dove viene messo in evidenza che l'effetto dell'Hadamard gate consiste nel mandare ciascuno stato della base standard in una sovrapposizione ripettivamente simmetrica e antisimmetrica degli stessi.
In Fig.2.2 è riportato il simbolo circuitale dell'Hadamard gate.

Figura 2.2: Simbolo circuitale dell'Hadamard gate.

CNOT: Controlled-NOT gate

Le trasformazioni su sistemi a più qubit possono essere costruite come prodotto tensoriale di trasformazioni a 1 qubit. Un esempio fondamentale di gate a più qubit è il Controlled-NOT gate, solitamente abbreviato in CNOT gate. Si tratta di un gate a 2 qubit che agisce sugli stati della base standard nel seguente modo:

$$\begin{aligned} C_{NOT} : |00\rangle &\rightarrow |00\rangle \\ |01\rangle &\rightarrow |01\rangle \\ |10\rangle &\rightarrow |11\rangle \\ |11\rangle &\rightarrow |10\rangle \end{aligned}$$

Il suo effetto è quello di invertire lo stato del secondo qubit solo nel caso in cui il primo qubit si trovi nello stato $|1\rangle$.
La rappresentazione spettrale del CNOT è

$$\begin{aligned} C_{NOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X = |0\rangle\langle 0| \otimes (|0\rangle\langle 0| + |1\rangle\langle 1|) + |1\rangle\langle 1| \otimes (|1\rangle\langle 0| + |0\rangle\langle 1|) = \\ |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| \,, \end{aligned}$$

mentre in termini di rappresentazione matriciale (nella base standard) si ha che

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Il CNOT gate ha un ruolo fondamentale nella realizzazione di stati entangled a partire da stati non entangled, come verrà mostrato nel prossimo capitolo.
Il simbolo circuitale del CNOT gate è riportato nella Fig.2.3.

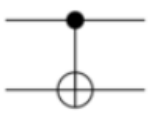


Figura 2.3: Simbolo circuitale del CNOT gate. Il qubit di controllo è contrassegnato dal tondo pieno.

Set universali di gate quantistici: operatori di rotazione, shift di fase e rotazione di fase

Finora sono stati presentati soltanto alcuni dei più utilizzati gate quantistici. In generale, qualsiasi gate quantistico a un qubit può essere espresso come combinazione di tre tipi di trasformazioni:

$$R(\beta) = \begin{pmatrix} \cos\beta & \sin\beta \\ -\sin\beta & \cos\beta \end{pmatrix}$$

$$K(\delta) = e^{i\delta} I$$

$$T(\alpha) = \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}$$

$K(\delta)$ rappresenta uno shift di fase globale, $R(\beta)$ una rotazione e $T(\alpha)$ una rotazione di fase. In termini di sfera di Bloch, $R(\beta)$ realizza una rotazione di un angolo β attorno all'asse y e $T(\alpha)$ una rotazione di un angolo α attorno all'asse z.

Presa una generica trasformazione unitaria ad un qubit Q, essa potrà essere espressa come

$$Q = K(\delta)T(\alpha)R(\beta)T(\gamma) = \begin{pmatrix} e^{i(\delta+\alpha+\gamma)}\cos\beta & e^{i(\delta+\alpha-\gamma)}\sin\beta \\ -e^{i(\delta-\alpha+\gamma)}\sin\beta & e^{i(\delta-\alpha-\gamma)}\cos\beta \end{pmatrix},$$

per opportuni $\alpha, \gamma, \beta, \delta$.

2.2 L'entropia di Shannon e l'informazione mutua

La teoria dell'informazione, sia classica sia quantistica, verte attorno a due obiettivi: dato un determinato messaggio, si vuole

(a) disporre di una grandezza in grado di descrivere fino a che livello il messaggio possa essere compresso senza perdere l'informazione in esso contenuta, ovvero quanto il messaggio sia ridondante;

(b) disporre di una grandezza che stabilisca la ridondanza necessaria a trasmettere fedelmente il messaggio attraverso un canale fisico affetto da rumore.

In questa sezione ci si concentrarà principalmente su come la prima questione venga risolta nel caso classico.

Si consideri una sorgente in grado di comporre messaggi sottoforma di stringhe di caratteri estratti a sorte tra quelli di un alfabeto $\aleph$ di k lettere, $\aleph = \{a_1, a_2, \ldots, a_k\}$, e si supponga che ogni lettera $a_x \in \aleph$ abbia probabilità a priori $p(a_x)$, $\sum_x^k p(a_x) = 1$, di apparire nel messaggio.
Considerando un messaggio con $n \gg 1$ caratteri preparato estraendo indipendentemente ciascun carattere dall'ensemble $X = \{a_x, p(a_x)\}$, l'entropia di Shannon di tale messaggio è definita come

$$H(X) \equiv \langle -\log_2 p(a_x) \rangle = \sum_x -p(a_x)\log_2 p(a_x) \tag{2.1}$$

e quantifica il numero di minimo di bit necessari a codificare l'informazione contenuta in ogni lettera del messaggio e quindi l'informazione comunicabile trasmettendo una singola

lettera estratta dall'ensemble.

Un utile esempio per approfondire questo aspetto è il caso dell'alfabeto binario.
Per n molto grande, è possibile applicare la legge dei grandi numeri: una tipica stringa prodotta da una sorgente che emette "0" con probabilità p e "1" con probabilità $1-p$ conterrà circa np "0" e $n(1-p)$ "1". Questo implica che il numero di stringhe tipiche distinte sarà dell'ordine del coefficiente binomiale $\binom{n}{np}$, che può essere stimato applicando l'approssimazione di Stirling[5] come segue:

$$\log_2 \binom{n}{np} = \log_2\left(\frac{n!}{(np)![n(1-p)]!}\right) = \log_2(n!) - \log_2((np)!) - \log_2((n-np)!) \simeq$$

$$\simeq n\log_2 n - n - np\log_2(np) + np - (n-np)\log_2(n-np) + n - np =$$

$$= n(-p\log p - (1-p)\log(1-p)),$$

dove si è sottintesa la base 2 del logaritmo.
Dato che per questo tipo di sorgente l'entropia di Shannon è proprio $H(p) = -p\log p - (1-p)\log(1-p)$, si ottiene che il numero di stringhe tipiche distinte è $2^{nH(p)}$.
Ne consegue che il codice che verrà impiegato per codificare il messaggio dovrà essere in grado di identificare univocamente ciascuna di queste stringhe al fine di trasmettere correttamente l'informazione in esse contenuta. Ciò può essere realizzato impiegando un codice che assegni un intero positivo ad ogni stringa tipica: tale "nuovo" alfabeto conterrà dunque $2^{nH(p)}$ lettere, ciascuna rappresentabile in binario con una stringa di lunghezza $nH(p)$. Tali lettere saranno inoltre equiprobabili a priori, essendo rappresentative di stringhe tipiche, quindi conterranno in media anche la stessa informazione.
Per quanto riguarda la compressione, dato che $0 \leq p \leq 1$, risulta che $0 \leq H(p) \leq 1$, con $H(p) = 1$ verificato solo nel caso in cui $p = 1/2$, perciò il messaggio risulta comprimibile ad un numero inferiore di bit ogni volta che "0" e "1" non sono equiprobabili.

Per alfabeti non binari, si ha analogamente che il numero di bit necessario a rappresentare un messaggio di n lettere è $nH(X)$, con X ensemble associato all'alfabeto. Ponendo $n = 1$, si ottiene che $H(X)$ rappresenta effettivamente l'informazione in bit contenuta mediamente in una singola lettera e dunque l'informazione trasmissibile a priori. Cosa accade però nel momento in cui il canale fisico di trasmissione è affetto da rumore?

In presenza di rumore, il messaggio inviato e quello ricevuto potrebbero non coincidere. Detti x e y rispettivamente i messaggi trasmessi e ricevuti e note le proprietà del canale di trasmissione, è possibile calcolare sfruttando la conoscenza relativa a y la probabilità condizionata $p(x|y)$ applicando il teorema di Bayes:

$$p(x|y) = \frac{p(y|x)p(x)}{p(y)}.$$

Nel caso in cui x e y siano correlati, la conoscenza di y può quindi portare ad una modifica delle probabilità a priori associate alle lettere dell'alfabeto e quindi modificare anche il numero di bit per lettera necessari alla codifica.
Esiste un'importante grandezza volta a quantificare proprio questa variazione: l'*informazione mutua*, definita come

$$I(X;Y) \equiv H(X) - H(X|Y) = H(Y) - H(Y|X), \tag{2.2}$$

[5] L'approssimazione di Stirling consente di esprimere $\log n!$ come $n\log n - n + O(\log n)$.

dove X, Y rappresentano gli ensemble relativi a x, y, mentre $H(X|Y) \equiv \langle -\log p(x|y) \rangle$, $H(Y|X) \equiv \langle -\log p(y|x) \rangle$ sono dette *entropie condizionate*.

Il ruolo dell'informazione mutua è di fornire una misura della correlazione tra messaggio trasmesso e messaggio ricevuto. Ovviamente nel caso in cui essi non siano correlati si ottiene che $I(X;Y) = 0$. Inoltre, in generale si ha che $I(X;Y) \geq 0$, dal momento che la conoscenza su y non può in alcun modo diminuire il grado di conoscenza su x.

L'informazione mutua costituisce anche una misura della quantità massima di informazione trasmissibile attraverso un canale rumoroso, noto a priori l'ensemble X.

2.3 L'entropia di Von Neumann

Il concetto di entropia classico è facilmente estendibile al caso quantistico supponendo che la sorgente componga i messaggi estraendo le lettere da un *ensemble di stati puri*. L'alfabeto nel caso quantistico diventa quindi un set di stati ρ_x, ciascuno con probabilità a priori p_x di essere utilizzato.
Dal momento che i caratteri che compongono il messaggio vengono emessi dalla sorgente seguendo le sole distribuzioni di probabilità, ogni lettera emessa sarà equivalente ad un sistema completamente descritto dall'operatore di densità

$$\rho = \sum_x p_x \rho_x.$$

e un messaggio di n stati avrà associato l'operatore $\rho \otimes \cdots \otimes \rho = \rho^n$.

L'entropia di Von Neumann per un operatore di densità ρ è definita come

$$S(\rho) = -\mathrm{tr}(\rho \log \rho). \tag{2.3}$$

L'entropia di Von Neumann coincide con l'entropia di Shannon nel momento in cui si adotta una base ortonormale che diagonalizzi ρ:

$$\rho = \sum_i \lambda_i |i\rangle\langle i| \implies S(\rho) = H(X), \tag{2.4}$$

con $X = \{i, \lambda_i\}$ ensemble per il calcolo dell'entropia di Shannon.

La relazione (2.4) offre uno spunto per una riflessione importante sulla distinguibilità. Nel caso classico, le lettere che compongono una stringa sono sempre distinguibili; nel caso quantistico invece le lettere sono veri e propri stati quantistici e pertanto non sono in generale distinguibili, lo sono solo nel momento in cui l'alfabeto è composto da una base ortonormale di stati puri, che sono tutti perfettamente distinguibili (mediante processi di misurazione di tipo PVM).

L'entropia di Von Neumann gode di una serie di proprietà che, come di vedrà nel prossimo capitolo, la rendono un'ottima candidata per quantificare l'entanglement:

(a) **Stati puri.** Uno stato puro $\rho = |\psi\rangle\langle\psi|$ ha entropia *nulla*.
Questo riflette il fatto che, per uno stato puro, la preparazione è unica, perciò non vi è alcun grado di ignoranza sul messaggio trasmesso;

(b) **Invarianza.** L'entropia è invariante per trasformazioni U unitarie: $S(U\rho U^{-1}) = S(\rho)$; [6]

(c) **Concavità.** Siano $\lambda_1, \ldots, \lambda_n$ coefficienti positivi tali per cui $\sum_{i=1}^{n} \lambda_i = 1$; allora

$$S\Big(\sum_{i=1}^{n} \lambda_i \rho_i\Big) \geq \sum_{i=1}^{n} \lambda_i S(\rho_i),$$

ovvero maggiore è il grado di ignoranza sullo stato di preparazione del sistema, maggiore è l'entropia;

(d) **Limite superiore.** Siano D gli autovalori non nulli di ρ; allora $S(\rho) \leq \log D$

(e) **Entropia di misurazione.** Si consideri un osservabile

$$A = \sum_y |a_y\rangle \, a_y \, \langle a_y| \,,$$

con probabilità $p(a_y) = \langle a_y|\rho|a_y\rangle$ che esso assuma il valore a_y in seguito ad una misurazione. L'ensemble dei possibili esiti di un'operazione di misura sarà $Y = \{a_y, p(a_y)\}$ e soddisferà la relazione

$$H(Y) \geq S(\rho),$$

con l'uguaglianza verificata per A, ρ commutanti. Questa proprietà è molto importante a livello fisico, perché indica che è possibile minimizzare il grado di aleatorietà del processo di misura andando a selezionare un osservabile commutante con l'operatore di densità;

(f) **Entropia di preparazione.** Sia $X = \{|\psi_x\rangle \, , p_x\}$ un ensemble di stati puri. Se il messaggio viene preparato estraendo uno stato puro in modo casuale da X, l'operatore di densità associato al sistema sarà

$$\rho = \sum_x p_x \, |\psi_x\rangle\langle\psi_x| \,,$$

e quindi l'entropia di Shannon associata a X risulta

$$H(X) \geq S(\rho),$$

con l'uguaglianza verificata per $|\psi_x\rangle$ ortogonali tra loro.
Questa disuguaglianza implica che la distinguibilità viene ridotta nel momento in cui si adotta un ensemble di stati non ortogonali;

(g) **Subadditività** Sia ρ_{AB} lo stato di un sistema bipartito AB. Allora

$$S(\rho^{AB}) \leq S(\rho^A) + S(\rho^B),$$

con ρ^A, ρ^B operatori di densità ridotti. L'entropia di Von Neumann dunque è additiva solo per sistemi non correlati; nel caso generale infatti parte dell'informazione sul sistema totale è contenuta anche nella correlazione tra i suoi sottosistemi, perciò l'entropia associata al sistema totale risulta inferiore rispetto alla somma delle sue parti, in perfetta analogia col caso classico.

[6] L'entropia dipende per definizione dalla traccia di $\rho \log \rho$ e dunque dai soli autovalori dell'operatore di densità, che sono invarianti per trasformazioni unitarie.

(h) **Subadditività forte** Per ogni sistema tripartito ρ^{ABC}, è verificata la relazione

$$S(\rho^{ABC}) + S(\rho^B) \leq S(\rho^{AB}) + S(\rho^{BC})$$

(i) **Disuguaglianza di Araki-Lieb** Per un sistema bipartito AB,

$$S(\rho^{AB}) \geq \left|S(\rho^A) - S(\rho^B)\right|.$$

Quest'ultima proprietà è fondamentale perché mette in evidenza una differenza molto importante tra entropia di Shannon e di Von Neumann: mentra nel caso classico l'entropia del sistema eccede sempre quella della singola parte, nel caso quantistico è possibile l'inverso. Si consideri infatti un sistema bipartito in uno stato puro: si ha che[7] $S(\rho^A) = S(\rho^B) \geq 0$, mentre $S(\rho^{AB}) = 0$. L'entropia nulla implica che non vi è alcun grado di ignoranza sullo stato di preparazione del sistema, ma questa conoscenza perfetta dello stato complessivo non influisce minimamente sui due sottosistemi, che continueranno a esibire un comportamento aleatorio in seguito ai processi di misura.
Questo vuol dire che non è possibile determinare lo stato del sistema osservando separatamente i suoi sottosistmei, ovvero che l'informazione è contenuta in correlazioni *non locali* tra di essi.

2.3.1 La compressione di Schumacher

Finora sono state elencate solo le proprietà prettamente "matematiche" dell'entropia di Von Neumann. La sua interpretazione in termini di informazione quantistica discende invece da un importante protocollo per la compressione dati: la *compressione di Schumacher*.

Nel caso quantistico, il termine "compressione" va interpretato come una riduzione della dimensione dello spazio di Hilbert associato al sistema.
In particolare, dalla compressione di Schumacher discende che per un messaggio di n lettere, $n \to \infty$, estratte dall'ensemble $\{|\psi_x\rangle, p_x\}$ di stati puri $|\psi_x\rangle$, non necessariamente ortogonali, è possibile comprimere lo spazio di Hilbert $\mathscr{H}$ ad esso associato fino alla dimensione

$$\log(dim\mathscr{H}) = nS(\rho), \tag{2.5}$$

dove $\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x|$.

La dimostrazione di quest'ultima relazione è particolarmente complessa e esula da questa trattazione, quindi se ne riportano solo le basi concettuali.[8].

La compressione di Schumacher costituisce una estensione al caso quantistico di quanto visto precedentemente per l'entropia di Shannon: l'idea sottostante è che per n molto grande, l'operatore di densità $\rho^n = \rho \otimes \cdots \otimes \rho$ abbia come supporto solo un sottospazio dello spazio di Hilbert complessivo associato ai messaggi.
Prendendo una base ortonormale che diagonalizzi ρ, dalla proprietà (f) dell'entropia di Von Neumann discende che la sorgente di informazione quantistica è trattabile come una sorgente effettivamente classica, perché i messaggi prodotti saranno stringhe di autostati di ρ, ciascuno con probabilità data dal prodotto dei corrispondenti autovalori e

[7] Le due quantità sono non nulle solo nel caso in cui lo stato puro sia entangled, come verrà specificato più avanti.

[8] Per una dimostrazione completa cfr. sezione 5.3.2 del capitolo 5 delle *Lecture Notes for Ph219/CS219: Quantum Information and Computation* [20].

perfettamente distinguibili l'uno dall'altro. La dimensione del sottospazio generato dagli autovettori di ρ^n tenderà asintoticamente a $2^{nS(\rho)}$, perciò sarà possibile codificare i messaggi limitatamente al sottospazio "tipico" mantendendo comunque ottima fedeltà di trasmissione per $n \to \infty$.

La relazione (2.5) permette dunque di interpretare $S(\rho)$ come il numero minimo di qubit per lettera necessari a trasmettere fedelmente un messaggio composto da stati quantistici puri e non necessariamente ortogonali.

2.3.2 L'informazione di Holevo

Nel caso degli stati misti, l'entropia di Von Neumann non è più interpretabile in termini di compressibilità. Se tuttavia l'alfabeto è composto da stati misti ortogonali fra loro, allora è possibile stimare il numero minimo di qubit necessario a codificarne le lettere attraverso l'*informazione di Holevo*.

Sia $\mathscr{E} = \{\rho_x, p_x\}$ un ensemble formato da stati misti e sia $\rho = \sum_x p_x \rho_x$ l'operatore di densità associato a ciascun carattere estratto casualmente dall'ensemble. Si definisce "informazione di Holevo" la quantità

$$\chi(\mathscr{E}) = S(\rho) - \sum_x p_x S(\rho_x). \tag{2.6}$$

Si noti che nel caso di un ensemble di stati puri, $\chi(\mathscr{E})$ si riduce all'entropia di Von Neumann di ρ.

L'informazione di Holevo presenta alcuni aspetti particolarmente interessanti. Innanzitutto, $\chi(\mathscr{E})$ tiene conto sia dell'operatore di densità del sistema sia di come esso viene costruito a partire dall'ensemble. L'informazione di Holevo quindi è un'indicatore di quanto il grado di conoscenza della preparazione dell'ensemble riduce l'entropia di Von Neumann e quindi costituisce un analogo quantistico dell'informazione mutua.

Un'altro aspetto interessante emerge quando si vanno a considerare stati misti ortogonali fra loro. In tal caso, è possibile scegliere una base che diagonalizza in forma di Jordan ρ e quindi di esplicitare $S(\rho)$ come

$$S(\rho) = \mathrm{tr}(\rho \log \rho) = -\sum_x \mathrm{tr}(p_x\rho_x)\log(p_x\rho_x) = -\sum_x p_x \underbrace{\mathrm{tr}(\rho_x)}_{=1} \log p_x - \sum_x p_x \mathrm{tr}(\rho_x)\log(\rho_x) =$$

$$= H(X) + \sum_x p_x S(\rho_x)$$

dove sono state applicate le proprietà del logaritmo di una matrice e il teorema di caratterizzazione dell'operatore di densità.
Applicando la definizione di informazione di Holevo risulta quindi che

$$H(X) = \chi(\mathscr{E})$$

ovvero l'informazione di Holevo è legata anche all'informazione classica che può essere codificata e recuperata da uno stato quantistico.

2.3.3 Informazione accessibile

Si consideri un stato quantistico x estratto dall'ensemble di stati puri $\mathscr{E} = \{|\psi_x\rangle, p_x\}$. Tale stato viene trasmesso e su di esso viene effettuato un processo di misura descritto da F_y, ottenendo un esito y. La probabilità ottenere y a partire da x è esprimibile come $p(x|y) = \langle\psi_x|F_y|\psi_x\rangle$. Costruendo un ensemble X come nel caso dell'equazione (2.4) e detto Y l'ensemble degli esiti della misura, è possibile calcolare la mutua informazione $I(X;Y)$ ottenuta tramite il processo di misura, applicandone la definizione (vedi equazione (2.2)).

L'informazione accessibile è definita come la massima informazione mutua ottenible attraverso un processo di misura:

$$\mathrm{Acc}(\mathscr{E}) = \max_{\{F_y\}} I(X;Y), \tag{2.7}$$

con $\{F_y\}$ classe dei processi di misura effettuabili sul messaggio ricevuto.

Per stati ortogonali, puri o misti che siano, risulta che

$$\mathrm{Acc}(\mathscr{E}) = H(X). \tag{2.8}$$

In presenza di tali stati è infatti possibile scegliere come operatore di misura il proiettore ortogonale $F_y = |\psi_y\rangle\langle\psi_y|$, che produce una probabilità condizionale $p(y|x) = \delta_{y,x}$. Ne deriva che $I(X;Y) = H(X)$ e quindi che per stati ortogonali è valida la relazione 2.8.

Passando al caso più generale degli stati non ortogonali, esistono due limiti fondamentali per l'informazione accessibile:

- in presenza di stati puri, $\mathrm{Acc}(\mathscr{E}) \leq S(\rho)$;
- in presenza di stati misti $\mathrm{Acc}(\mathscr{E}) \leq \chi(\mathscr{E})$, noto come *limite di Holevo*.

Capitolo 3

Entanglement

L'entanglement è considerato uno degli aspetti più nonclassici del formalismo quantistico e deve la sua comparsa nel panorama della fisica agli scienziati Einstein, Podolsky e Rosen, che nel 1935 lo utilizzarono all'interno del loro celebre articolo *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* [9].

Proprietà peculiare dei sistemi composti, l'entanglement si riscontra nella relazione tra i sottosistemi che compongono un dato sistema quantomeccanico. Tale relazione si manifesta in presenza di particolari stati, i cosiddetti stati *entangled*, e lo fa sia in forma di correlazioni tra osservabili dei singoli sottosistemi, non simulabili attraverso alcun formalismo classico, sia in termini di informazione. Una caratteristica molto importante degli stati entangled riguarda infatti l'informazione che forniscono su sistema complessivo e sottosistemi: l'informazione sul sistema complessivo risulta essere superiore a quella sui singoli sottosistemi.

Queste proprietà sono alla base di alcuni fenomeni chiave della teoria dell'informazione quantistica (la crittografia quantistica, il quantum dense coding, il teletrasporto quantistico) e rendono l'entanglement una risorsa fondamentale per la comunicazione quantistica. L'entanglement infatti può essere manipolato, trasmesso, controllato e distribuito [12], consentendo la realizzazione di una vasta gamma di protocolli quantistici, che vanno dalla riduzione della complessità della comunicazione classica alla simulazione del comportamento di sistemi quantistici.
Tuttavia, tali protocolli necessitano nella maggior parte dei casi di quantificare il grado di entanglement dello stato del sistema e quindi di una nozione di *misura* per l'entanglement.

Nel corso di questo capitolo verranno mostrate alcune delle misure di entanglement note in letteratura, precedute da un'introduzione sull'informazione quantistica, e quindi sui sistemi a più qubit, e dalla definizione formale di entanglement.
I concetti esposti faranno riferimento per la sezione 3.1 principalmente al capitolo 3 del testo *Quantum Computing. A Gentle Introduction* [22], al capitolo 4 delle dispense di *Quantum Information and Computation* di John Preskill [19] e all'articolo «Quantum entanglement» di R. Horodecki *et al.*[12]. Per la sezione 3.2, i testi di riferimento sono gli stessi della precedente, con l'aggiunta del capitolo 12 di *Quantum Computation and Quantum Information* [17].

3.1 La definizione di entanglement

La definizione di entanglement è posta in negativo: uno stato puro di un sistema composto è detto entangled se *non* è possibile esprimerlo come prodotto tensoriale di stati dei suoi sottosistemi, ovvero se dato $|\psi\rangle \in H$, con $H = \otimes_{k=1}^{n} H_k$ spazio di Hilbert,

$$\nexists\, |\psi_1\rangle \in H_1, \ldots, |\psi_n\rangle \in H_n \quad \text{t.c.} \quad |\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle\,.$$

Uno stato misto ρ invece è detto entangled se *non* è rappresentabile come combinazione convessa di prodotti tensoriali di stati, ovvero se

$$\nexists\, p_1, p_2, \ldots \quad \text{t.c.} \quad \rho = \sum_i p_i \rho_1^i \otimes \cdots \otimes \rho_n^i.$$

Inoltre, si parla di stati massimamente entangled quando preso un sistema composto, ad esempio il sistema bipartito AB, gli operatori di densità ridotti ρ^A, ρ^B risultano pari al prodotto di uno scalare per i rispettivi operatori identità I_A, I_B.

La definizione di entanglement così come è stata riportata non offre un criterio immediato per stabilire se un generico stato $|\phi\rangle$ sia entangled oppure separabile e nella maggior parte dei casi risolvere questo problema risulta particolarmente difficile.

Il caso degli stati puri di sistemi bipartiti è uno dei pochi in cui è possibile individuare una grandezza che permetta di discernere la separabilità o meno di uno stato: il *numero di Schmidt*.
Dato un sistema bipartito AB nello stato puro $|\psi\rangle$ con decomposizione di Schmidt

$$|\psi\rangle = \sum_i \lambda_i \,|i_A\rangle\,|i_B\rangle\,, \tag{3.1}$$

il numero di Schmidt è definito come il numero di autovalori non nulli (contandone la molteplicità) dell'operatore di densità ridotto ρ^A, o equivalentemente di ρ^B.
I due operatori ridotti risultano infatti essere nella forma

$$\rho^A = \sum_i \lambda_i^2 \,|i_A\rangle\langle i_A|\,, \quad \rho^B = \sum_i \lambda_i^2 \,|i_B\rangle\langle i_B|\,,$$

perciò i loro autovalori non nulli equivalgono al numero di termini della combinazione lineare (3.1). Ne deriva che gli stati con numero di Schmidt uguale ad 1 sono effettivamente esprimibili come prodotto tensoriale di stati dei singoli sottosistemi A, B e risultano quindi separabili. In presenza di numero di Schmidt maggiore di 1, lo stato non è più decomponibile in prodotto tensoriale ed è quindi uno stato entangled.

Dal momento che ogni stato puro dispone di una decomposizione di Schmidt (vedi Teorema 3), il numero di Schimidt costituisce per questa categoria di stati un criterio molto efficace, perché comporta solo una semplice diagonalizzazione degli operatori di densità ridotti.

3.1.1 Gli stati di Bell

L'esempio più semplice di stati entangled, e massimamente entangled, sono gli stati di Bell, detti anche *coppie EPR*[1]:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \quad |\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad |\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{3.2}$$

Considerando infatti il prodotto tensoriale $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + b_1a_2|10\rangle + b_1b_2|11\rangle$, è immediato notare come non esistano a_1, a_2, b_1, b_2 coefficienti complessi non nulli tali per cui il risultato del prodotto tensoriale corrisponda ad uno degli stati di Bell, perciò tali stati sono non separabili.
Il fatto che siano massimamente entanglement si dimostra invece andando ad applicare le definizioni di operatore di densità ridotto e di traccia parziale (equazioni (1.19) e (1.20)). Considerando un sistema composto da due qubit A, B preparato nello stato $|\Phi^+\rangle$, si ha che

$$\begin{aligned} \rho^A &= \mathrm{tr}_B(|\Phi^+\rangle\langle\Phi^+|) = \frac{1}{2}\mathrm{tr}_B(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|) = \\ &= \frac{1}{2}\Big(|0\rangle\langle 0|_A \underbrace{\langle 0|0\rangle_B}_{=1} + |0\rangle\langle 1|_A \underbrace{\langle 0|1\rangle_B}_{=0} + |1\rangle\langle 0|_A \underbrace{\langle 1|0\rangle_B}_{=0} + |1\rangle\langle 1|_A \underbrace{\langle 1|1\rangle_B}_{=1}\Big) = \frac{1}{2}I_A, \end{aligned}$$

e procedendo in modo analogo si ottiene che $\rho^B = \frac{1}{2}I_B$.

Gli stati di Bell si contraddistinguono per due proprietà fondamentali:

- costituiscono una base per lo spazio di Hilbert di un sistema a due qubit;
- l'entropia associata agli operatori di densità ridotti ρ^A, ρ^B è $S(\rho^A) = S(\rho^B) = 1$.

Inoltre, hanno rivestito un ruolo fondamentale nello sviluppo delle prime teorie riguardanti l'entanglement. La loro importanza può essere colta attraverso un esperimento mentale ideato dal fisico David Bohm a partire dal paradosso EPR.
Immaginiamo che venga creata da una sorgente luminosa una coppia di fotoni nello stato $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ e che poi ciascun fotone venga inviato a due osservatori arbitrariamente lontani A e B. Ogni osservatore potrà effettuare misurazioni solo sul proprio fotone.
Se A effettua una misura rispetto alla base standard e ottiene l'esito $|0\rangle$, lo stato complessivo del sistema collasserà in $|00\rangle$. Quindi, se B effettua in seguito una misura sulla propria particella, osserverà anch'esso lo stato $|0\rangle$. La situazione sarebbe perfettamente analoga anche se fosse B il primo ad effettuare la misura o se l'esito ottenuto da A fosse $|1\rangle$.
Sostanzialmente, emerge che le misurazioni sui singoli qubit sono sempre correlate, ma gli sperimentatori ne sono consapevoli solo se si comunicano vicendevolmente gli esiti. In mancanza di comunicazione, ciò che entrambi osservano è un comportamento perfettamente random, in cui le probabilità di ottenere $|0\rangle$ e $|1\rangle$ sono entrambe 1/2.

Nel caso di stati massimamente entangled di sistemi bipartiti è possibile dunque con un'unica misurazione determinare lo stato di entrambi i qubit, noto lo stato complessivo. Questa proprietà è particolarmente interessante nell'ottica di una computazione basata

[1] Dagli scienziati Einstein, Podolsky e Rosen.

sui qubit. In presenza di entanglement massimizzato è sufficiente infatti effettuare una sola misurazione per conoscere lo stato di tutti i qubit, mentre nel caso classico è necessario verificare in successione lo stato di *ogni* bit per poter determinare l'esito della computazione.
L'entanglement tra stati quindi è fondamentale per poter realizzare una computazione quantistica efficiente.

A livello circuitale, come era stato anticipato nella scorsa sezione è possibile ottenere mediante trasformazioni unitarie uno stato entangled a partire da uno stato di base. Consideriamo ad esempio lo stato di Bell $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Questo stato è ottenibile a partire dal ket di base $|00\rangle$ applicando prima una trasformazione di Hadamard al primo qubit e poi una trasformazione CNOT:

$$C_{NOT}(H(|0\rangle)\,|0\rangle) = C_{NOT}(\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\,|0\rangle) = C_{NOT}(\frac{1}{\sqrt{2}}(|00\rangle+|10\rangle)) = \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle). \tag{3.3}$$

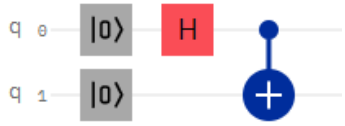


Figura 3.1: Schema circuitale delle trasformazioni descritte dall'equazione (3.3).

Un'applicazione degli stati di Bell: il teletrasporto quantistico

Un protocollo molto impiegato in teoria dell'informazione quantistica, e che verrà utilizzato anche in questa trattazione, è il *teletrasporto quantistico*.
Si tratta di un protocollo che sfrutta una coppia di Bell[2] per trasmettere con fedeltà ottimale uno stato quantistico $|\psi\rangle$ da un osservatore A ad un osservatore B arbitrariamente lontano. La peculiarità della trasmissione è che essa avviene su canali *classici* di comunicazione: l'osservatore B infatti con questo tipo di protocollo ricostruisce lo stato che si vuole copiare a partire dall'informazione classica che riceve dall'osservatore A.

Vediamo innanzitutto il caso in cui lo stato $|\psi\rangle$ è nella generica forma $a\,|0\rangle + b\,|1\rangle$. Per teletrasportare tale stato sono sufficienti 5 operazioni:

(a) A e B, prima di allontanarsi, preparano un sistema a due qubit in uno stato di Bell, ad esempio $|\Phi^+\rangle$, per poi prendere un qubit ciascuno senza effettuare *alcuna* misurazione;

(b) B si allontana, mentre A entra in possesso di un ulteriore qubit C nello stato $|\psi\rangle$;

(c) A effettua una misura congiunta sul sistema AC, formato dal suo qubit e da quello appena preparato, in modo da proiettare lo stato di AC su uno dei quattro stati di Bell ($|\Phi^{\pm}\rangle_{CA}\,, |\Psi^{\pm}\rangle_{CA}$); l'esito della misura può essere codificato classicamente impiegando 2 bit (è sufficiente infatti associare un numero binario ad ogni stato di Bell);

(d) A invia a B, attraverso un canale classico, il risultato ottenuto;

[2]Con "coppia di Bell" si intende una coppia di qubit che si trovano in uno dei 4 stati di Bell.

(e) B, a seconda dell'informazione ricevuta, effettua una delle trasformazioni di Pauli sul proprio qubit.

Vediamo perché queste operazioni producono effettivamente un teletrasporto.
Lo stato complessivo del sistema dopo il punto (b) è

$$|\psi\rangle_C |\Phi^+\rangle_{AB} = (a|0\rangle_C + b|1\rangle_C)(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B)\frac{1}{\sqrt{2}} =$$

$$= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle),$$

che può essere espresso in termini di stati di Bell come

$$\begin{aligned} &= \frac{1}{2}|\Phi^+\rangle_{CA}(a|0\rangle_B + b|1\rangle_B) + \frac{1}{2}|\Psi^+\rangle_{CA}(a|1\rangle_B + b|0\rangle_B + \\ &+ \frac{1}{2}|\Psi^-\rangle_{CA}(a|1\rangle_B - b|0\rangle_B) + \frac{1}{2}|\Phi^-\rangle_{CA}(a|0\rangle_B - b|1\rangle_B). \end{aligned} \tag{3.4}$$

Ora, notando che le quattro parentesi tonde racchiudono rispettivamente l'effetto delle trasformazioni di Pauli $I, X, -Y, Z$ su $|\psi\rangle_B$, si può comprendere l'importanza del punto (e) del protocollo. Infatti, la misurazione effettuata da A determina il collasso equiprobabile del sistema in uno dei termini dell'equazione (3.4), perciò B per ottenere lo stato $|\psi\rangle_B$ altro non deve fare che eseguire sul proprio qubit la corrispondente trasformazione di Pauli. Bisogna ricordare infatti che $X^2 = -Y^2 = Z^2 = I$, perciò applicando la corretta trasformazione di Pauli (univocamente determinata dall'informazione classica ricevuta) è possibile per B riottenere lo stato $|\psi\rangle$ a partire dal proprio qubit.

Il teletrasporto quantistico è generalizzabile anche a stati di sistemi N dimensionali [4]. In tal caso però il sistema bipartito condiviso da A e B deve essere nella forma

$$|\Phi\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|j\rangle \otimes |j\rangle,$$

con j che indica gli elementi di una base ortonormale per lo spazio di Hilbert associato al sistema.
Si noti che $|\Phi\rangle$ è comunque uno stato massimamente entangled.
Nel caso generale dunque A e B non impiegano più qubit, bensì particelle a N stati e le operazioni di misura e manipolazioni di tali stati saranno più complesse.
L'operatore di misura adottato da A dovrà infatti avere autostati del tipo

$$|\varphi_{nm}\rangle = \frac{1}{\sqrt{N}}\sum_j e^{(2\pi i)\frac{jn}{N}}|j\rangle \otimes |j+m\rangle,$$

con j, m t.c. $0 \leq j + m \leq N - 1$, mentre trasformazioni unitarie eseguite da B sulla propria particella entangled dipenderanno dall'esito nm e saranno nella forma

$$U_{nm} = \sum_k e^{(2\pi i)\frac{kn}{N}}|k\rangle\langle k+m|,$$

con k t.c. $0 \leq k + m \leq N - 1$.

3.1.2 Entanglement e località

La procedura per ottenere un semplice stato entangled, riassunta dall'equazione (3.3), mette in luce uno degli aspetti chiave dell'entanglement: il fatto che esso non possa essere creato né tantomeno alterato solo attraverso trasformazioni unitarie locali, ovvero applicate sui singoli sottosistemi.
Per ottenere lo stato di Bell $|\Phi^+\rangle$, nell'esempio riportato al termine della scorsa sottosezione si era infatti resa necessaria l'applicazione di una trasformazione a due qubit: il CNOT gate.
L'entanglement si presenta quindi ancora una volta come un fenomeno intrinsecamente basato sulla interazione tra le parti che compongono un sistema.

A livello matematico, questo aspetto viene confermato in modo evidente dal numero di Schmidt.
A inizio capitolo il numero di Schmidt era stato introdotto come valido criterio per stabilire la separabilità di uno stato. Essendo il numero di Schmidt dipendente dagli autovalori degli operatori di densità ridotti, si ha che esso non può essere alterato da trasformazioni unitarie, perché esse godono della proprietà di lasciare invariati gli autovalori degli operatori.

Questo particolare legame dell'entanglement con le trasformazioni locali diventa fondamentale nel momento in cui si vuole trovare una misura in grado di quantificare l'entanglement, perché impone la proprietà di invarianza per trasformazioni unitarie locali.

3.2 Misurare l'entanglement

Si è fatto riferimento più volte al fatto che la definizione di entanglement, essendo posta in negativo, renda piuttosto ostica una trattazione precisa e rigorosa del fenomeno.
Uno degli aspetti più difficoltosi riguarda proprio trovare una misura in grado di quantificare in modo efficace il grado di entanglement di uno stato.
L'entanglement infatti assume innanzitutto sfumature diverse a seconda dello stato e del tipo di sistema che si sta trattando: la definizione stessa è diversa a seconda che si stiano trattando stati puri o stati misti e non è affatto immediato stabilire come confrontare stati di sistemi bipartiti diversi, ad esempio uno formato da due qubit con uno formato da due qutrit[3].

Per comparare sistemi diversi, in generale è buona norma trovare innanzitutto una unità di misura comune e poi individuare le trasformazioni in grado di confrontare ciascun sistema con l'unità comune.
Nel caso dell'entanglement, si può già affermare che tali trasformazioni dovranno essere locali e unitarie (vedi la sezione 3.1.2). Si considereranno in particolare le trasformazioni LOOC, dall'inglese *Local Operations and Classical Communication*. Si tratta di una particolare classe di trasformazioni che comprende trasformazioni locali, ovvero applicate ai singoli sottosistemi, e che ammette che i vari sottosistemi comunichino tra loro mediante informazione classica.
Un esempio di LOOC è proprio il teletrasporto quantistico.

[3] I qutrit sono sistemi isolati a tre livelli.

Non tutte le LOOC sono applicabili a stati entangled: esiste infatti un teorema[4], che mi limito a riportare senza dimostrazione, che restringe il pool di possibili trasformazioni relativamente allo stato di partenza e allo stato di arrivo.

Teorema 5. *Siano $|\psi\rangle, |\varphi\rangle$ due stati puri del sistema bipartito AB. Definiti i due operatori di densità ridotti*

$$\rho_\psi = tr_B(|\psi\rangle\langle\psi|), \quad \rho_\varphi = tr_B(|\varphi\rangle\langle\varphi|),$$

è possibile trasformare $|\psi\rangle$ in $|\varphi\rangle$ tramite LOOC se e solo se $\lambda_\psi \leq \lambda_\varphi$, dove $\lambda_\psi, \lambda_\varphi$ sono le somme degli autovalori (molteplicità compresa) di ρ_ψ, ρ_φ.

Una misura di entanglement $E(\rho)$, con ρ generico operatore di densità, per essere ben definita dovrà rispettare una serie di requisiti minimi, che consentano di mantenere una compatibilità con le proprietà dell'entanglement messe in luce nelle scorse sezioni. Tali criteri sono riassunti in [26] e comprendono:

(a) $E(\rho) \geq 0$, con l'uguaglianza verificata solo nel caso in cui ρ rappresenta uno stato separabile;

(b) $E(\rho)$ rimane invariata per trasformazioni locali;

(c) il valore di aspettazione di $E(\rho)$ non aumenta in presenza di trasformazioni LOOC;

(d) $E(\rho)$ deve essere convessa, ovvero $\sum_i p_i E(\rho_i) \geq E(\sum_i p_i \rho_i)$;[5]

(e) $E(\rho)$ deve essere monotona.

Per estrapolare alcune delle principali misure di entanglement si procederà nel seguente modo: si considererà innanzitutto un caso particolare relativamente semplice, gli stati puri bipartiti, per poi estendere la trattazione agli stati puri in generale e successivamente agli stati misti.

3.2.1 Stati puri bipartiti: il legame con l'entropia di Von Neumann

Sia $|\psi\rangle_{AB}$ lo stato puro bipartito di cui si vuole valutare l'entanglement e si adotti come unità di misura uno stato massimamente entangled, ad esempio $|\Phi\rangle^+ = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Per quantificare l'entanglement dello stato in esame si procede in modo asintotico, ovvero considerando un numero $n \to \infty$ di copie di $|\psi\rangle_{AB}$ e valutando poi il numero massimo k_{max} di copie di $|\Phi^+\rangle$ estraibili tramite LOOC dalle n copie e il numero minimo k_{min} di copie di $|\Phi^+\rangle$ necessario a creare n copie di $|\psi\rangle_{AB}$.
A priori sappiamo che $k_{max} \geq k_{min}$, ma dimostrando che

$$\lim_{n\to\infty} \frac{k_{min}}{n} = \lim_{n\to\infty} \frac{k_{max}}{n},$$

è possibile definire l'entanglement di $|\psi\rangle_{AB}$ come

$$E(|\psi\rangle_{AB}) \equiv \lim_{n\to\infty} \frac{k_{min}}{n} = \lim_{n\to\infty} \frac{k_{max}}{n} = S(\rho^A) = S(\rho^B). \tag{3.5}$$

[4]Per la dimostrazione completa cfr. capitolo 12.5.1, Teorema 12.15 del testo *Quantum Comupation and Quantum Information*[17].

[5]Questo criterio secondo [12] non è strettamente necessario, ma è comunque una proprietà matematica conveniente.

Dimostrazione. Si consideri direttamente la decomposizione di Schmidt $|\psi\rangle_{AB} = \sum_i \sqrt{p_i}\,|i\rangle_A\,|i\rangle_B$.
Il sistema complessivo formato dalle n copie sarà esprimibile come

$$|\psi\rangle^{\otimes n} = \sum_{i_1,\dots,i_n} \sqrt{p_{i_1}\dots p_{i_n}}\,|i_{1_A} i_{2_A}\dots i_{n_A}\rangle\,|i_{1_B} i_{2_B}\dots i_{n_B}\rangle \;\in\; H^{\otimes n},$$

con $H^{\otimes n} = H_1 \otimes \cdots \otimes H_n$.
Si effettui ora una compressione di Schumacher: escludendo i termini relativi agli stati non ϵ-tipici[6], si ottiene la riduzione di $H^{\otimes n}$ ad uno spazio di Hilbert di dimensione

$$\log\Big(\dim \tilde{H}^{\otimes n}\Big) = n(S(\rho^A) + \epsilon),$$

con conseguente riduzione dello stato a

$$|\tilde{\psi}^{\otimes n}\rangle = \sum_{\epsilon-\text{tipici}} \sqrt{p_{i_1}\dots p_{i_n}}\,|i_{1_A} i_{2_A}\dots i_{n_A}\rangle\,|i_{1_B} i_{2_B}\dots i_{n_B}\rangle\,,$$

che dovrà poi essere opportunamente normalizzato. Si lavorerà quindi direttamente sulla versione normalizzata, che sarà indicata con $|\tilde{\psi}_1^{\otimes n}\rangle$.
Si considerino adesso due sperimentatori A e B che condividono $k = n(S(\rho^A) + \epsilon)$ stati di Bell (ciascuno può lavorare localmente solo su uno dei due qubit che compongono lo stato). Per fare in modo che essi condividano al termine dell'esperimento n copie di $|\psi\rangle_{AB}$, sarà sufficiente sfruttare le k copie di stati di Bell per effettuare un teletrasporto quantistico, in cui A prepara localmente sia la parte di $|\tilde{\psi}_1^{\otimes n}\rangle$ che rimarrà in suo possesso sia la parte che poi trasmetterà a B sfruttando gli stati di Bell. Per ottenere lo stato $|\psi\rangle$ iniziale basterà poi decomprimere $|\tilde{\psi}_1^{\otimes n}\rangle$.
Nel limite di $n \to \infty$, essendo ϵ una costante piccola a piacere, si ottiene che

$$\lim_{n\to\infty} \frac{k_{min}}{n} = \frac{k}{n} = \frac{nS(\rho^A)}{n} = S(\rho^A).$$

Per ricavare la seconda parte dell'equazione (3.5) si procede in modo simile. Si supponga che A e B condividano n copie di $|\psi\rangle$.
Sarà possibile per A trasformare $|\psi\rangle^{\otimes n}$ in $|\tilde{\psi}_1^{\otimes n}\rangle$ mediante una misurazione sul sottospazio delle sequenze ϵ-tipiche.
Dato che la probabilità di ottenere una sequenza ϵ-tipica misurando lo stato $|\psi\rangle^{\otimes n}$ è al massimo $2^{-n(S(\rho^A)-\epsilon)}$, il massimo coefficiente di Schmidt che potrà apparire in $|\tilde{\psi}_1^{\otimes n}\rangle$ sarà di $2^{-n(S(\rho^A)-\epsilon)/2}/\sqrt{1-\delta}$.[7]
Il massimo autovalore possibile associato a $\rho_{\tilde{\psi}} = \mathrm{tr}_B\left|\tilde{\psi}_1^{\otimes n}\right\rangle\!\left\langle\tilde{\psi}_1^{\otimes n}\right|$ sarà dunque $2^{-n(S(\rho^A)-\epsilon)}/(1-\delta)$.
Scegliamo una costante k' tale per cui

$$\frac{2^{-n(S(\rho^A)-\epsilon)}}{1-\delta} \leq 2^{-k'}.$$

In virtù del Teorema 5, sarà possibile trasformare lo stato associato a $\rho_{\tilde{\psi}}$ in un stato ρ' con tutti gli autovalori pari a $k' \approx nS(\rho^A)$, nel limite $\epsilon, \delta \to 0$, $n \to \infty$.
Dato che gli stati di Bell hanno la peculiarità di avere $S(\rho^A) = 1$, lo stato ρ' sarà realizzabile tramite un ensemble di k' stati Bell.
Di conseguenza, si ottiene che

[6]Con ϵ-tipico si intende uno stato la cui probabilità $p_{i_1}\dots p_{i_n}$ di essere ottenuto è compresa tra $2^{-n(S(\rho_A)+\epsilon)}$ e $2^{-n(S(\rho_A)-\epsilon)}$.

[7]Il fattore $\sqrt{1-\delta}$, con δ costante piccola a piacere, va inserito per tenere conto degli effetti dell'operazione di normalizzazione sui coefficienti di Schmidt.

$$\lim_{n\to\infty} \frac{k_{max}}{n} = \frac{k'}{n} = \frac{nS(\rho^A)}{n} = S(\rho^A),$$

come volevasi dimostrare.

□

Si noti che con questa definizione, la misura risulta ben definita rispetto ai criteri riportati a inizio sezione. Questo discende dalle proprietà matematiche dell'entropia di Von Neumann nel caso degli stati puri.

I due protocolli impiegati nella dimostrazione consentono di derivare due misure di entanglement valide anche per stati misti biparti: l'*entanglement di formazione* e l'*entanglement di distillazione*.
Il primo si basa sulla quantità di risorse (in unità di stati di Bell) impiegate per la creazione dello stato entangled e quindi può essere espresso come

$$F(\rho^{AB}) = \lim_{n\to\infty} \frac{k_{min}}{n}.$$

L'entanglement di distillazione adotta invece come unità di misura il numero di risorse estraibili dallo stato entangled (in unità di stati di Bell). Per uno stato misto bipartito, risulta immediato esprimerlo come

$$D(\rho^{AB}) = \lim_{n\to\infty} \frac{k_{max}}{n}.$$

3.2.2 Il caso generale: la misura geometrica e la *convex roof construction*

L'entanglement di formazione e di distillazione sono solo due delle svariate misure di entanglement che si possono ritrovare nella letteratura. Una rassegna piuttosto completa è contenuta in [12].

Entanglement di formazione e di distillazione sono molto utili per mostrare alcune delle considerazioni necessarie ad estrapolare una forma di misura di entanglement, ma si prestano poco alla generalizzazione agli stati puri di sistemi multipartiti. Esiste tuttavia un'ulteriore misura in grado di facilitare questa generalizzazione: la *misura geometrica*.

La misura geometrica di entanglement si basa per l'appunto su considerazioni di tipo geometrico: l'idea fondamentale è valutare l'entanglement di uno stato in termini di "lontananza" dallo stato separabile più vicino.
Occorre però definire in modo più rigoroso il concetto di lontananza: si definisce misura geometrica dell'entanglement di uno stato $|\psi\rangle$ (bipartito e non) la quantità

$$E_g(|\psi\rangle) \equiv \min_{|\phi_s\rangle}(1 - |\langle\psi|\phi_s\rangle|^2) = 1 - \max_{|\phi_s\rangle} |\langle\psi|\phi_s\rangle|^2, \tag{3.6}$$

con $\{|\phi_s\rangle\}$ famiglia di stati separabili [26, 11]. Si noti che il processo di minimizzazione/massimizzazione su $\{|\phi_s\rangle\}$ è assolutamente non banale e non sempre può essere valutato analiticamente [26].

L'estensione agli stati misti si effettua con il metodo della *convex roof construction*. Questo tipo di estensione può essere fatta a partire da una qualsiasi misura per stati puri e consiste nella seguente definizione. Sia

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \,, \quad \sum_i p_i = 1,$$

l'operatore di densità associato ad uno stato misto. Si definisce entanglement di ρ la quantità

$$E(\rho) = \min \sum_i p_i E(|\psi_i\rangle), \tag{3.7}$$

dove $E(|\psi_i\rangle)$ rappresenta una misura di entanglement per stati puri.

La convex roof contruction consiste quindi in una minimizzazione su tutte le possibili decomposizioni in stati puri dell'operatore di densità ρ.
Ovviamente anche questa definizione dovrà soddisfare i criteri riportati a inizio sezione. Una dimostrazione per il caso della costruzione a partire da E_g è disponibile in [26].

Capitolo 4

Quantificare l'entanglement di uno stato misto: il protocollo proposto da Kuzmak e Tkachuk

Nell'articolo «Measuring entanglement of a rank-2 mixed state prepared on a quantum computer» [1], A. R. Kuzmak e V. M. Tkachuk presentano un protocollo per calcolare l'entanglement di stati misti di rango 2.
Si tratta di una coppia di procedure volte a quantificare l'entanglement: una analitica e una sperimentale basata su computer quantistico.

Questo capitolo sarà articolato in due parti. Nella prima verranno presentate le basi teoriche della procedura analitica, ovvero come sia ricabile una formula esatta per l'entangled geometrico di un sistema misto a partire dalla definizione stessa di entanglement geometrico.
Nella seconda parte verrà invece mostrato in che modo è possibile sfruttare un computer quantistico per valutare in forma approssimata e sperimentale l'entanglement geometrico.

Entrambe le sezioni sono basate principalmente sugli articoli «Quantifying geometric measure of entanglement by mean value of spin and spin correlations with application to physical systems», di A.Frydryszak, M. Samar e V. Tkachuk [11], e «Measuring entanglement of a rank-2 mixed state prepared on a quantum computer», di V.M. Tkachuk e A.R. Kuzmak [1].

4.1 Le basi teoriche e il protocollo analitico

Il protocollo proposto in [1] è stato sviluppato per misurare l'entanglement di un certo qubit rispetto al resto del sistema nel caso in cui tale sistema si trovi in uno stato misto di N qubit di rango 2, il cui stato è descritto dalla matrice di densità

$$\rho = \sum_a \omega_a \left|\psi_a\right\rangle\!\left\langle\psi_a\right|, \tag{4.1}$$

dove $|\psi_a\rangle$ sono stati puri descritti da combinazioni lineari di $|\vec{0}\rangle = |00\ldots0\rangle$ e $|\vec{1}\rangle = |11\ldots1\rangle$, con $\sum_a \omega_a = 1$.

L'idea alla base del protocollo è di individuare delle grandezze medie in grado di caratterizzare l'entanglement del sistema. La necessità di lavorare con dei valori medi deriva

dal comportamento aleatorio delle misure in meccanica quantistica: i risultati forniti da un computer quantistico sono infatti delle distribuzioni di probabilità di ottenere ciascuno stato di base in seguito ad una misurazione.
Su questo aspetto poi si tornerà più avanti.

In [1], queste quantità medie vengono individuate nei valori medi dei seguenti due operatori:

$$\Sigma^x = \sigma_1^x \sigma_2^x \dots \sigma_i^x \dots \sigma_N^x,$$
$$\Sigma^y = \sigma_1^x \sigma_2^x \dots \sigma_i^y \dots \sigma_N^x,$$

dove il pedice i indica il qubit di cui si vuole valutare l'entanglement rispetto al resto del sistema.
Si tratta di operatori formati dal prodotto di N operatori di Pauli, ognuno agente sullo stato del corrispondente qubit (σ^x, σ^y corrispondono rispettivamente alle matrici σ_1, σ_2 riportate in (1.18)).
I valori medi dei due operatori si calcolano applicando la relazione (1.2), che per lo stato (4.1) assume la forma

$$\langle \Sigma^k \rangle = \sum_a \omega_a \langle \psi_a | \Sigma^k | \psi_a \rangle , \quad k = x, y, \tag{4.2}$$

e consentono di esprimere l'entanglement dell'i-esimo qubit rispetto al resto del sistema come

$$E(\rho) = \frac{1}{2}\Big(1 - \sqrt{1 - \langle \Sigma^x \rangle^2 - \langle \Sigma^y \rangle^2}\Big). \tag{4.3}$$

Vediamo in che modo è possibile ottenere questa relazione a partire dalla misura geometrica di entanglement.

Si consideri un sistema con N qubit. Un generico stato puro di un sistema formato da un primo qubit entagled con il resto del sistema può essere rappresentato come

$$|\psi\rangle = a\,|0\rangle\,|\phi_1\rangle + b\,|1\rangle\,|\phi_2\rangle\,,$$

dove $|\phi_1\rangle\,, |\phi_2\rangle$ sono vettori di stato arbitrari (unitari ma non necessariamente ortogonali) e rappresentanti il resto dei qubit del sistema.
È possibile esprimere $|\psi\rangle$ con una combinazione lineare di stati ortogonali impiegando la seguente decomposizione di Schmidt:

$$|\psi\rangle = \lambda_1\,|c_1\rangle\,|\tilde{\phi}_1\rangle + \lambda_2\,|c_2\rangle\,|\tilde{\phi}_2\rangle\,, \tag{4.4}$$

dove $\langle \tilde{\phi}_1 | \tilde{\phi}_2 \rangle = 0$ e

$$|c_1\rangle = \frac{|0\rangle + c\,|1\rangle}{\sqrt{1 + |c|^2}}, \quad |c_2\rangle = \frac{c^*\,|0\rangle - |1\rangle}{\sqrt{1 + |c|^2}},$$

con c costante complessa opportuna.
Essendo (4.4) una decomposizione di Schmidt, dal Teorema 3 sappiamo che λ_1, λ_2 sono due coefficienti reali che soddisfano $\lambda_1^2 + \lambda_2^2 = 1$.

Andiamo ora a valutare l'entanglement geometrico di $|\psi\rangle$.
La misura geometrica dipende dal massimo della sovrapposizione tra lo stato in esame e un set di stati puri non entangled. In questo caso è immediato prendere come set di stati l'insieme $\{|c_1\rangle\,|\tilde{\phi}_1\rangle\,, |c_2\rangle\,|\tilde{\phi}_2\rangle\}$. Questi stati infatti, oltre ad essere puri e separabili, sono anche ortogonali fra loro e sappiamo che

$$\langle \psi | (|c_1\rangle\,|\tilde{\phi}_1\rangle)\rangle = \lambda_1, \quad \langle \psi | (|c_2\rangle\,|\tilde{\phi}_2\rangle)\rangle = \lambda_2,$$

perciò discende dall'equazione (3.6) che

$$E(|\psi\rangle) = 1 - \max(\lambda_1^2, \lambda_2^2).$$

Si consideri ora l'operatore di Pauli $\vec{\sigma}$ agente sul primo qubit del sistema. Il suo valore medio è legato ai coefficienti di Schmidt [11] come

$$\langle\vec{\sigma}\rangle^2 = (\lambda_1^2 - \lambda_2^2)^2 = (1 - 2\lambda_1^2)^2 = (1 - 2\lambda_2^2)^2,$$

espressione che permette di esprimere entrambi i coefficienti di Schmidt in funzione di un unico valore medio:

$$\lambda_{1,2}^2 = \frac{1}{2}(1 \pm |\langle\vec{\sigma}\rangle|).$$

Per un generico stato puro quindi la misura geometrica di entanglement risulta

$$E(|\psi\rangle) = \frac{1}{2}(1 - |\langle\vec{\sigma}\rangle|). \tag{4.5}$$

In presenza di un sistema fisico, quale ad esempio un sistema di spin, questo vuol dire che è possibile valutare l'entanglement del primo spin rispetto al resto del sistema andando semplicemente a misurarne il valor medio.[1].

Consideriamo ora un sistema a 2 qubit nello stato misto

$$\rho = \sum_i p_i \, |\psi_i\rangle\langle\psi_i| \, ,$$

con $|\psi_i\rangle$ combinazioni lineari degli stati $|\Uparrow\rangle \equiv |00\rangle \, , |\Downarrow\rangle \equiv |11\rangle$.

Ogni $|\psi_i\rangle$ sarà esprimibile nel linguaggio della sfera di Bloch come

$$|\psi_i\rangle = \cos\frac{\theta_i}{2} \, |\Uparrow\rangle + e^{i\varphi_i} \sin\frac{\theta_i}{2} \, |\Downarrow\rangle \, .$$

Considerando il sottospazio generato da $|\Uparrow\rangle \, , |\Downarrow\rangle$, è possibile estendervi il formalismo di Pauli introducendo i tre operatori

$$\Sigma^x = \sigma_1^x \sigma_2^x, \quad \Sigma^y = \sigma_1^y \sigma_2^x, \quad \Sigma^z = \sigma_1^z I_2. \tag{4.6}$$

Questi tre operatori infatti agiscono su $|\Uparrow\rangle$ e $|\Downarrow\rangle$ esattamente come gli operatori di Pauli agiscono su $|0\rangle \, , |1\rangle$:

$$\Sigma^x \, |\Uparrow\rangle = \sigma_1^x \, |0\rangle \, \sigma_2^x \, |0\rangle = |1\rangle \, |1\rangle = |\Downarrow\rangle \, ;$$

$$\Sigma^x \, |\Downarrow\rangle = \sigma_1^x \, |1\rangle \, \sigma_2^x \, |1\rangle = |0\rangle \, |0\rangle = |\Uparrow\rangle \, ;$$

da cui

$$\Sigma^x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

e si dimostra analogamente che

$$\Sigma^y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \Sigma^z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

[1]Deriva dal fatto che l'operatore associato allo spin è $\vec{S} = \frac{\hbar}{2}\vec{\sigma}$, perciò $\langle\vec{S}\rangle = \frac{\hbar}{2}\langle\vec{\sigma}\rangle$.

A questo punto, è possibile estendere la rappresentazione (1.17) agli stati puri $|\psi_i\rangle$ come

$$\rho_i = \frac{1 + \vec{r_i} \cdot \vec{\Sigma}}{2}, \quad |\vec{r_i}| = 1,$$

che permette di esprimere lo stato misto complessivo come

$$\rho = \sum_i p_i \rho_i = \frac{1 + \sum_i p_i \vec{r_i} \cdot \vec{\Sigma}}{2}.$$

Se si pone $\sum_i p_i \vec{r_i} = \vec{r}$, si ottiene un operatore di densità analogo a ρ_i, che quindi differisce da uno stato puro solo per il modulo di $\vec{r}$ ($|\vec{r}| \leq 1$ con l'uguaglianza verificata solo per uno stato puro).

Per valutare l'entanglement dello stato misto occorre procedere secondo il metodo della *convex roof construction*, perciò prima occorrerà calcolare $E(|\psi_i\rangle)$ e poi applicare la relazione (3.7).

Dall'equazione (4.5) sappiamo che l'entanglement del primo qubit rispetto al resto del sistema, nel caso di uno stato puro, dipende solo dal valore di aspettazione dell'operatore di Pauli $\vec{\sigma}_1$. Si procede quindi valutando i seguenti valori medi:

$$\langle\psi_i|\sigma_1^x|\psi_i\rangle = (\cos\frac{\theta_i}{2}\langle 00| + e^{-i\varphi_i}\sin\frac{\theta_i}{2}\langle 11|)(\cos\frac{\theta_i}{2}|10\rangle + e^{i\varphi_i}\sin\frac{\theta_i}{2}|01\rangle) = 0$$

$$\langle\psi_i|\sigma_1^y|\psi_i\rangle = (\cos\frac{\theta_i}{2}\langle 00| + e^{-i\varphi_i}\sin\frac{\theta_i}{2}\langle 11|)(i\cos\frac{\theta_i}{2}|10\rangle - ie^{i\varphi_i}\sin\frac{\theta_i}{2}|01\rangle) = 0$$

$$\langle\psi_i|\sigma_1^z|\psi_i\rangle = (\cos\frac{\theta_i}{2}\langle 00| + e^{-i\varphi_i}\sin\frac{\theta_i}{2}\langle 11|)(\cos\frac{\theta_i}{2}|00\rangle - e^{i\varphi_i}\sin\frac{\theta_i}{2}|11\rangle) = \cos^2(\frac{\theta_i}{2}) - \sin^2(\frac{\theta_i}{2}) =$$

$$= \cos\left(2\frac{\theta_i}{2}\right) = \cos\theta_i$$

dove è stata sfruttata l'ortonormalità della base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Quindi, applicando l'equazione (4.5) si ottiene che

$$E(|\psi_i\rangle) = \frac{1}{2}(1 - |\langle\psi_i|\sigma_1^z|\psi_i\rangle|) = \frac{1}{2}(1 - |\cos\theta_i|) = \frac{1}{2}(1 - |r_i^z|), \tag{4.7}$$

con l'ultima uguaglianza ricavata notando che, essendo $\vec{r_i}$ unitario, $\cos\theta_i$ individua la componente lungo l'asse z di $\vec{r_i}$, indicata con r_i^z.

Applichiamo ora la relazione (3.7):

$$E(\rho) = \min\sum_i p_i E(|\psi_i\rangle) = \frac{1}{2}(1 - \max\sum_i p_i |r_i^z|). \tag{4.8}$$

Per calcolare l'entanglement dello stato misto occorre dunque fare una massimizzazione non banale su tutte le possibili decomposizioni in stati puri dell'operatore di densità. Notiamo innanzitutto che, essendo $\vec{r_i}$ unitario e $\sum_i p_i = 1$, si ha che

$$\sum_i p_i |\vec{r_i}| = 1.$$

Questa relazione consente di esprimere il problema di massimizzazione in modo più agevole, ponendo $\vec{k_i} = p_i\vec{r_i}$: trovare

$$\max\sum_i |k_i^z|, \tag{4.9}$$

con condizioni

$$\sum_i \vec{k}_i = \vec{r}, \tag{4.10}$$

$$\sum_i \left|\vec{k}_i\right| = 1. \tag{4.11}$$

Si tratta di un problema affrontabile da un punto di vista puramente geometrico: i vincoli (4.10), (4.11) possono essere interpretati come una fune inestensibile, di lunghezza unitaria, le cui estremità sono fissate agli estremi di $\vec{r}$, che si ricorda avere modulo inferiore ad 1 in presenza di stati misti. Il problema di massimizzazione equivale quindi a modificare la disposizione spaziale della fune in modo tale da otterne la massima proiezione sull'asse z.
Non tutte le deformazioni sono consentite: la fune ha lunghezza fissata, perciò tutte le possibili deformazioni descrivono un ellisse i cui fuochi coincidono con gli estremi di $\vec{r}$. Si sta escludendo volutamente una trattazione tridimensionale, perché ciò che interessa è esclusivamente la massima proiezione lungo z, perciò è sufficiente considerare il piano generato da $\vec{r}$ e dall'asse z (vedi Fig.4.1).

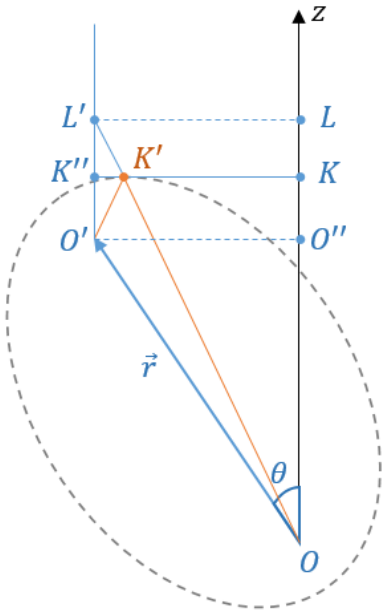


Figura 4.1: Costruzione geometrica impiegata in [11] per valutare la quantità (4.9).

Ora, per risolvere il problema (4.9) si procede realizzando la costruzione riportata in Fig.4.1. Si fissa l'origine dell'asse z in uno dei due fuochi e si considera sull'ellisse il punto K', tale per cui la tangente all'ellisse in K' risulta perpendicolare all'asse z. Tale tangente individua la proiezione OK lungo l'asse z del segmento OK', che è la massima proiezione ottenibile per un segmento congiungente O e un punto qualsiasi dell'ellisse.
In questo caso, i vettori $\vec{k}_i$ sono soltanto due: $\overrightarrow{OK'}$ e $\overrightarrow{K'O'}$. Di conseguenza,

$$\max \sum_i |k_i^z| = |O''K| + |O'K''|. \tag{4.12}$$

La quantità (4.12) può essere espressa in funzione dei soli $\vec{r}$ e θ facendo delle ulteriori considerazioni.
Si consideri il prolungamento $K'L'$ del segmento OK'. I due triangoli $O'K'K''$, $K'K''L$

sono congruenti[2], pertanto si ha che $|O''K|+|O'K''| = |OL|$ e che $|OL'| = |L'K'|+|O'K'| = |O'K'| + |OK'| = 1$, perciò

$$|OL| = \sqrt{1 - |LL'|^2} = \sqrt{1 - |O'O''|} = \sqrt{1 - r^2 \sin^2 \theta}.$$

In coordinate cartesiane, $r^2 \sin^2 \theta$ equivale a $r_x^2 + r_y^2$, perciò si ottiene che

$$E(\rho) = \frac{1}{2}\Big(1 - \sqrt{1 - r_x^2 - r_y^2}\Big). \tag{4.13}$$

Valutiamo ora $\langle \Sigma^x \rangle$. Per la relazione (1.16),

$$\langle \Sigma^x \rangle = \mathrm{tr}(\Sigma^x \rho),$$

quindi ricordando che ρ è nella forma

$$\rho = \frac{1 + \vec{r} \cdot \vec{\Sigma}}{2}$$

e che

$$\Sigma^x \Sigma^x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \quad \Sigma^x \Sigma^y = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i\Sigma^z, \quad \Sigma^x \Sigma^z = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -i\Sigma^y,$$

si ottiene che

$$\langle \Sigma^x \rangle = \frac{1}{2}\mathrm{tr}\Big(\Sigma^x + r_x I + i r_y \Sigma^z - i r_z \Sigma^y\Big) = \frac{1}{2} 2 r_x = r_x,$$

dove è stata sfruttata la linearità della traccia e il fatto che le matrici $\Sigma^x, \Sigma^y, \Sigma^z$ hanno traccia nulla.
Con un procedimento analogo, si ottiene che

$$\langle \Sigma^y \rangle = r_y,$$

quindi andando a sostituire queste due relazioni nella (4.13), si ricava l'equazione (4.3).

La dimostrazione è stata effettuata per un sistema a 2 qubit e nel caso in cui il qubit rispetto a cui calcolare l'entanglement sia il primo, ma è perfettamente generalizzabile al caso dell'i-esimo qubit di un sistema a N qubit. È sufficiente prendere $|\Uparrow\rangle = |00\ldots0\rangle$, $|\Downarrow\rangle = |11\ldots1\rangle$ e considerare come componenti di $\vec{\Sigma}$

$$\Sigma^x = \sigma_1^x \sigma_2^x \ldots \sigma_N^x, \quad \Sigma^y = \sigma_1^x \sigma_2^x \ldots \sigma_i^y \ldots \sigma_N^x, \Sigma^z = I_1 I_2 \ldots \sigma_i^z \ldots I_N.$$

4.2 Il protocollo sperimentale

La relazione (4.3) dimostrata nella scorsa sezione è una formula *esatta* per valutare l'entanglement geometrico di un sistema. Tale formula tuttavia richiede un lavoro analitico non indifferente per calcolare i vari valori medi.
Nell'articolo [1] viene mostrato come sia possibile stimare l'entanglement sperimentalmente, con il supporto di un computer quantistico.

[2]Sono congruenti per il secondo criterio di congruenza dei triangoli: il lato $K'K''$ è in comune, gli angoli $\widehat{O'K''K'}, \widehat{L'K''K'}$ sono congruenti perché entrambi retti e anche gli angoli $\widehat{L'K'K''}, \widehat{O'K'K''}$ sono congruenti, perché $\widehat{L'K'K''} \cong \widehat{OK'K}$ (sono opposti al vertice) e $\widehat{O'K'K''} \cong \widehat{OK'K}$ (proprietà della tangente ad un punto di un ellisse).

Prima di presentare la parte legata al protocollo, è opportuno ricordare brevemente il funzionamento di un computer quantistico.

La caratteristica fondamentale di un computer quantistico è che esso ha alla base sistemi fisici assimilabili a qubit. Ad oggi sono state implementate varie tipologie di qubit, basate principalmente su cinque tipi di sistemi fisici, le cui caratteristiche sono riportate e messe a confronto in Fig.4.2.

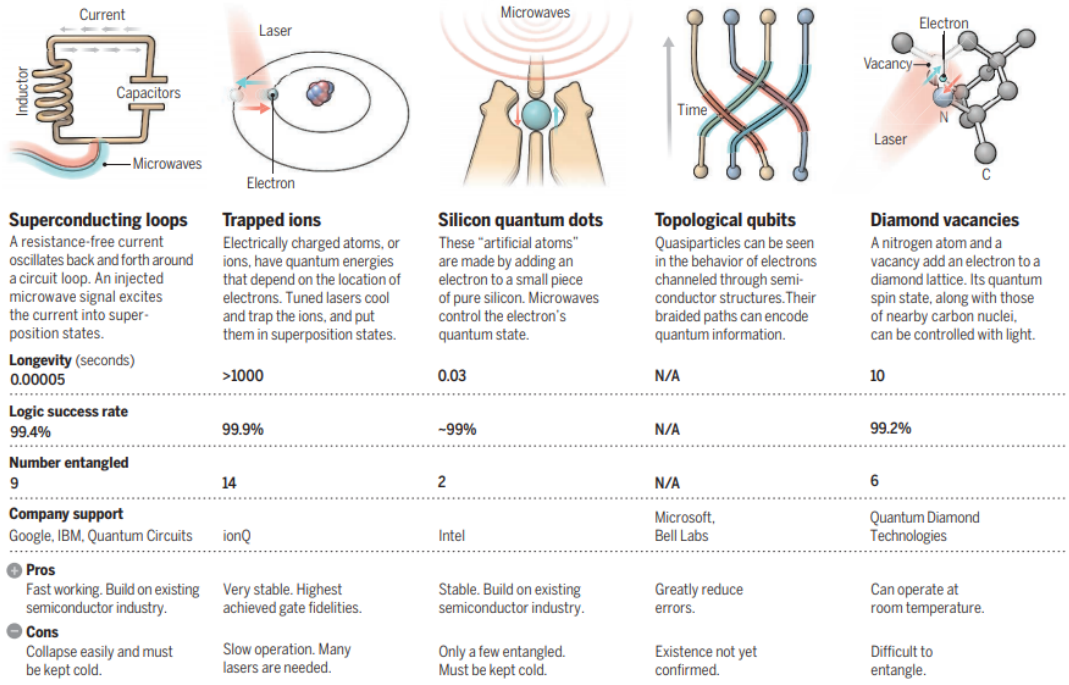


Figura 4.2: Stato dell'arte (2016) delle principali tecniche di implementazione di qubit. Per ciascuna tipologia è riportata una breve descrizione della fisica del sistema adottato, il tempo di coerenza degli stati, il rate di successo delle operazioni logiche, il numero massimo di qubit che possono trovarsi in stati entangled, i pro e i contro. Fonte: G.Popkin (2016) [18].

La computazione avviene tipicamente così: si inizializza lo stato del sistema di qubit ad uno stato di fiducia $|00\ldots0\rangle$ e si applicano ad esso una serie di trasformazioni unitarie, ovvero dei gate quantistici. Infine, si effettua una misura dello stato di uno o più qubit lungo gli autostati $|0\rangle, |1\rangle$ dell'operatore di Pauli σ^z.
Nel caso di un sistema di spin, quest'ultima operazione equivale a trovare ciascuno spin nello stato $|\uparrow\rangle$ o nello stato $|\downarrow\rangle$.
Preparando un numero sufficientemente elevato di copie dello stato $|00\ldots0\rangle$ ed effettuando le stesse manipolazioni, è possibile stimare le probabilità di trovare il sistema in ciascuno stato di base dopo la misurazione. Come precisato nella sezione 1.2.1, queste probabilità sono legate ai coefficienti che identificano univocamente lo stato di un sistema, perciò possono essere usate per ricostruire lo stato ottenuto tramite le manipolazioni.

Queste procedure, per fornire dei risultati attendibili, impongono alcuni requisiti sui sistemi fisici usati per la computazione. Questi requisiti sono espressi da cinque condizioni, note come *criteri di DiVincenzo*[3][13, 7]: un computer quantistico, per potersi definire tale

[3]Dal nome del fisico teorico David P. DiVincenzo, che per primo propose questi criteri.

deve

(a) essere un sistema fisico scalabile con qubit ben caratterizzati;

(b) avere l'abilità di inizializzare lo stato dei qubit ad un semplice stato di fiducia, ad esempio $|00\ldots0\rangle$;

(c) avere tempi di decoerenza molto maggiori del tempo necessario ai gate per eseguire le proprie operazioni;

(d) disporre un set universale di gate quantistici implementabile;

(e) garantire la possibilità di leggere selettivamente lo stato dei qubit.

Il requisito di elevati tempi di decoerenza deriva dal fatto che l'interazione dei qubit con l'ambiente, inevitabile in un apparato reale, può causare una dispersione dell'informazione quantistica nell'ambiente. Questo fenomeno, detto per l'appunto *decoerenza*, andrebbe ad inficiare i processi di computazione effettuati sui qubit, che si basano fortemente sull'evoluzione unitaria dei sistemi quantistici isolati.
Per un qubit, le possibili fonti di decoerenza sono essenzialmente due: il *rilassamento* e il *dephasing*. Il rilassamento consiste nel collasso della funzione d'onda nello stato di base $|0\rangle$ e può essere pensato come l'equivalente dell'emissione spontanea di quanti di energia in un sistema a due livelli che si trova nello stato eccitato. Il dephasing, invece, riguarda variazioni della fase relativa di una sovrapposizione.

In un computer quantistico, i qubit devono necessariamente interagire con altre componenti hardware del sistema, ad esempio per lettura dei qubit e per il controllo delle trasformazioni applicate agli stati. Queste operazioni di solito sono gestite attraverso computer classici.

Al fine di produrre risultati affidabili, il computer deve essere tenuto innanzitutto a temperature inferiori ad 1 K, in modo da ridurre al minimo gli effetti di rumore termico, e deve disporre anche di tecniche di *quantum error correction* in grado di isolare e correggere eventuali errori senza perturbare lo stato dei qubit.

Vediamo ora come sfruttare un computer quantistico per misurare l'entanglement di un sistema.

Si è detto che il computer quantistico fornisce la probabilità di trovare ciascun qubit in uno degli autostati di σ^z. I due operatori Σ^x, Σ^y dipendono però dall'azione sui qubit di σ^x e σ^y.
È necessario dunque esprimere σ^x e σ^y in funzione di σ^z. Questa trasformazione si effettua facilmente impiegando l'*esponenziale di Pauli*:

$$\exp\left\{i\frac{\theta}{2}\vec{k}\cdot\vec{\sigma}\right\} = \cos\left(\frac{\theta}{2}\right)I + i\sin\left(\frac{\theta}{2}\right)\vec{k}\cdot\vec{\sigma}, \tag{4.14}$$

con $\vec{k}$ vettore unitario a tre componenti, I operatore identità e $\vec{\sigma}$ operatore di Pauli.
L'esponenziale di Pauli gode di una proprietà per cui, dati $\vec{v}, \vec{u}$ unitari,

$$\exp\left\{i\frac{\theta}{2}\vec{k}\cdot\vec{\sigma}\right\}\vec{u}\cdot\vec{\sigma}\exp\left\{-i\frac{\theta}{2}\vec{k}\cdot\vec{\sigma}\right\} = \vec{v}\cdot\vec{\sigma}, \tag{4.15}$$

dove

$$\cos\theta = \vec{v}\cdot\vec{u}, \quad \vec{k} = \frac{\vec{v}\wedge\vec{u}}{|\vec{v}\wedge\vec{u}|}.$$

Per ricavare σ^y in funzione di σ^z occorre quindi porre $\vec{v} = (0,1,0)$, $\vec{u} = (0,0,1)$. Applicando la (4.15) si ottiene che

$$\cos\theta = 0, \quad \vec{k} = (1,0,0),$$

perciò

$$\sigma^y = e^{i\frac{\pi}{4}\sigma^x}\sigma^z e^{-i\frac{\pi}{4}\sigma^x}.$$

Analogamente, ponendo $\vec{v} = (1,0,0)$, $\vec{u} = (0,0,1)$, si ha che

$$\sigma^x = e^{-i\frac{\pi}{4}\sigma^y}\sigma^z e^{i\frac{\pi}{4}\sigma^y}.$$

Gli operatori Σ^x, Σ^y a questo punto prendono la forma

$$\Sigma^x = e^{-i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots+\sigma_i^y+\ldots+\sigma_N^y)}\sigma_1^z\sigma_2^z\ldots\sigma_i^z\ldots\sigma_N^z e^{+i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots+\sigma_i^y+\ldots+\sigma_N^y)}$$

$$\Sigma^y = e^{-i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots-\sigma_i^x+\ldots+\sigma_N^y)}\sigma_1^z\sigma_2^z\ldots\sigma_i^z\ldots\sigma_N^z e^{+i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots-\sigma_i^x+\ldots+\sigma_N^y)}.$$

Possiamo quindi sfruttare questa rappresentazione per esprimere i valori medi degli operatori solo rispetto a σ_k^z. Infatti se poniamo

$$|\tilde{\psi}_a^x\rangle = e^{+i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots+\sigma_i^y+\ldots+\sigma_N^y)}|\psi_a\rangle, \quad |\tilde{\psi}_a^y\rangle = e^{+i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\ldots-\sigma_i^x+\ldots+\sigma_N^y)}|\psi_a\rangle,$$

che sono trasformazioni unitarie esprimibili come rotazioni di $\pi/2$ attorno all'asse y o x a seconda dell'operatore di Pauli coinvolto, ricaviamo che i valori medi (4.2) possono essere espressi come:

$$\langle\Sigma^k\rangle = \sum_a \omega_a \langle\tilde{\psi}_a^k|\sigma_1^z\sigma_2^z\ldots\sigma_i^z\ldots\sigma_N^z|\tilde{\psi}_a^k\rangle, \quad k = x,y. \tag{4.16}$$

Dato che l'azione di σ^z consiste nel trasformare $|0\rangle$ in $|0\rangle$ e $|1\rangle$ in $-|1\rangle$, all'atto della misurazione l'osservabile legato a σ^z assumerà valore ±1 a seconda dello stato misurato. Nel caso di un sistema a più qubit, questo comporta che uno stato di base contente nessuno o un numero pari di 1 (ad esempio $|0011\rangle$) avrà valore $+1$, mentre in caso di numeri dispari avrà valore -1.
Per stimare (4.16) è dunque sufficiente calcolare la probabilità di misurare ciascuno stato di base a partire da $|\tilde{\psi}_a^k\rangle$, moltiplicare tali probabilità per ±1 a seconda del valore associato allo stato e poi sommarle:

$$\langle\Sigma^k\rangle = \sum_a \omega_a(p_{a_{+1}}^k - p_{a_{-1}}^k), \quad k = x,y.$$

In termini di computazione quantistica, questo procedimento si traduce in:

(a) effettuare una serie di trasformazioni unitarie per ottenere $|\psi_a\rangle$ a partire da $|00\ldots0\rangle$;

(b) applicare le opportune rotazioni di $\pi/2$ a ciascun qubit del sistema;

(c) misurare lo stato di ogni qubit;

(d) per ricreare uno stato misto, fissare un numero X di iterazioni ed eseguire poi i precedenti punti $\omega_a X$ volte per ogni $|\psi_a\rangle$.

La realizzazione in termini di circuito quantistico dei punti (a)-(c) è riportata in Fig.4.3.

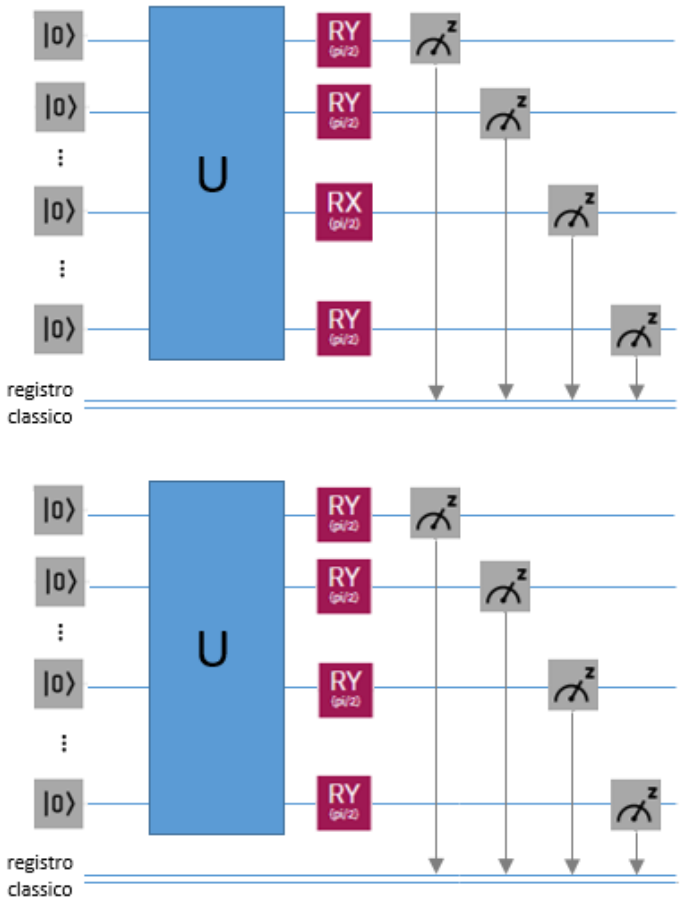


Figura 4.3: Schemi generali dei circuito per stimare $\langle\psi_a|\Sigma^k|\psi_a\rangle$. Il blocco U rappresenta tutte le trasformazioni necessarie a portare $|00\ldots0\rangle$ in $|\psi_a\rangle$. I blocchi RX e RY rappresentano le rotazioni di $\pi/2$ attorno agli assi x e y. Il circuito in alto è relativo a $k = y$, mentre quello in basso, perfettamente analogo, è relativo a $k = x$.

Capitolo 5

Implementazione del protocollo per un sistema a 4 qubit

Nel precedentemente capitolo è stato presentato il protocollo proposto da A.R. Kuzmak e V.M. Tkachuk per calcolare l'entanglement di un sistema di qubit che si trova in uno stato misto di rango 2.
In questo capitolo verranno mostrati i risultati da me ottenuti applicando il protocollo ad un sistema a 4 qubit.
Tali risultati comprendono sia l'entanglement del primo qubit rispetto al resto del sistema calcolato con la formula esatta ricavata nello scorso capitolo, sia il calcolo svolto tramite computer quantistico. Come computer quantistico ho utilizzato `ibmq_santiago`, uno dei dispositivi accessibili attraverso la piattaforma IBM Quantum Experience, sviluppata dall'azienda statunitense IBM.

Il capitolo sarà diviso in due parti: una prima sezione sarà dedicata al calcolo analitico, mentre la seconda ospiterà la parte relativa al computer quantistico e comprenderà un'introduzione alle funzionalità di base di Qiskit, il software sviluppato dall'IBM per permettere ai propri utenti di interfacciarsi con una piattaforma cloud di quantum computing, seguita da una descrizione del programma scritto da me su Qiskit per riprodurre la parte sperimentale del protocollo.
I risultati ottenuti dal procedimento analitico e da quello computazionale verranno poi confrontati nella parte finale del capitolo.

Per la stesura della parte relativa e Qiskit, è stata utilizzata la documentazione fornita dall'IBM, reperibile presso [25, 2], che ho poi integrato con *Learn Quantum Computation Using Qiskit* [3] e *IBM's Qiskit Tool Chain: Working with and Developing for Real Quantum Computers* [27].

5.1 Lo stato misto di rango 2 e il calcolo analitico

Come stato a cui applicare il protocollo ho scelto lo stesso stato analizzato in [1], in modo da poter poi confrontare i risultati con quelli riportati nell'articolo e avere quindi un feedback sulla correttezza del programma da me implementato tramite Qiskit.
Lo stato misto di rango 2 in questione è:

$$\rho_{exp} = \omega \left|\psi_+\right\rangle\!\left\langle\psi_+\right| + (1-\omega) \left|\psi_-\right\rangle\!\left\langle\psi_-\right|, \tag{5.1}$$

dove $\omega \in [0,1]$ e $|\psi_\pm\rangle = \frac{1}{\sqrt{2}}(|0000\rangle \pm |1111\rangle)$.
Si tratta dunque di uno stato misto di un sistema a 4 qubit il cui ensemble è costruito a partire da due soli stati puri, $|\psi_\pm\rangle$.

La funzione del parametro ω è determinare se l'accuratezza del protocollo sperimentale sia sensibile a variazioni della composizione dell'ensemble dello stato misto. Il parametro ω infatti rappresenta la percentuale di stato $|\psi_+\rangle$ contenuta nell'ensemble.

Per valutare l'accuratezza del procollo sperimentale ho prima calcolato l'entanglement del primo qubit rispetto agli altri tre in funzione di ω, in modo da avere un andamento teorico con cui confrontare i dati sperimentali. Poi, ho effettuato una simulazione tramite Qiskit, così da verificare che calcolo analitico e dati fossero, in assenza di rumore, compatibili. Infine, ho effettuato una serie di misurazioni con il computer quantistico `ibmq_santiago`, variando ω, e ho valutato gli errori associati a ciascuna misura.
In questa sezione riporto la parte analitica e l'espressione per l'entropia di entanglement $E(\rho_{exp})$ del primo qubit rispetto al resto del sistema da me ottenuta.

Per poter applicare la formula (4.3), ho calcolato innanzitutto i valori medi $\langle\Sigma^x\rangle, \langle\Sigma^y\rangle$. Per la relazione (4.2) si ha che

$$\begin{aligned} \langle\Sigma^x\rangle &= \omega \langle\psi_+|\Sigma^x|\psi_+\rangle + (1-\omega)\langle\psi_-|\Sigma^x|\psi_-\rangle, \\ \langle\Sigma^y\rangle &= \omega \langle\psi_+|\Sigma^y|\psi_+\rangle + (1-\omega)\langle\psi_-|\Sigma^y|\psi_-\rangle, \end{aligned} \tag{5.2}$$

ma dalla relazione (4.16) so che posso calcolare i valori medi semplicemente valutando l'azione di $\sigma_1^z\sigma_2^z\sigma_3^z\sigma_4^z$ su $|\tilde{\psi}_\pm^x\rangle$ e $|\tilde{\psi}_\pm^y\rangle$, dove

$$\begin{aligned} |\tilde{\psi}_\pm^x\rangle &= e^{i\frac{\pi}{4}(\sigma_1^y+\sigma_2^y+\sigma_3^y+\sigma_4^y)}|\psi_\pm\rangle, \\ |\tilde{\psi}_\pm^y\rangle &= e^{i\frac{\pi}{4}(-\sigma_1^x+\sigma_2^y+\sigma_3^y+\sigma_4^y)}|\psi_\pm\rangle. \end{aligned} \tag{5.3}$$

Occorre quindi ricavare in primis $|\tilde{\psi}_\pm^x\rangle$ e $|\tilde{\psi}_\pm^y\rangle$.
I calcoli completi sono riportati nell'appendice, di seguito mostro soltanto i passaggi principali per derivare $|\tilde{\psi}_+^x\rangle$, mentre per $|\tilde{\psi}_+^y\rangle$ e $|\tilde{\psi}_-^{x,y}\rangle$ riporto direttamente le espressioni ottenute.

Ricordando che

$$e^{i\frac{\pi}{4}\sigma^y} = \cos\frac{\pi}{4}I + i\sin\frac{\pi}{4}\sigma^y = \frac{1}{\sqrt{2}}(I + i^2|1\rangle\langle 0| - i^2|0\rangle\langle 1|) = \frac{1}{\sqrt{2}}(I - |1\rangle\langle 0| + |0\rangle\langle 1|),$$

si ha che

$$|\tilde{\psi}_+^x\rangle = \Big(\frac{1}{\sqrt{2}}\Big)^5 (I_1+i\sigma_1^y)(I_2+i\sigma_2^y)(I_3+i\sigma_3^y)(I_4+i\sigma_4^y)\Big(|0\rangle_1|0\rangle_2|0\rangle_3|0\rangle_4 + |1\rangle_1|1\rangle_2|1\rangle_3|1\rangle_4\Big)$$

da cui, svolgendo i calcoli, si ottiene che

$$|\tilde{\psi}_+^x\rangle = \frac{1}{2\sqrt{2}}\Big(|0\rangle + |3\rangle + |5\rangle + |6\rangle + |9\rangle + |10\rangle + |12\rangle + |15\rangle\Big),$$

dove gli stati di base sono stati espressi nella forma decimale.
Analogamente si ottiene che

$$|\tilde{\psi}_-^x\rangle = \frac{-1}{2\sqrt{2}}\Big(|1\rangle + |2\rangle + |4\rangle + |7\rangle + |8\rangle + |11\rangle + |13\rangle + |14\rangle\Big).$$

Per quanto riguarda $|\tilde{\psi}_+^y\rangle$, si ottiene che

$$|\tilde{\psi}_+^y\rangle = \frac{1}{4}\Big(e^{i\frac{7\pi}{4}}|0\rangle + e^{i\frac{5\pi}{4}}|1\rangle + e^{i\frac{5\pi}{4}}|2\rangle + e^{i\frac{7\pi}{4}}|3\rangle + e^{i\frac{5\pi}{4}}|4\rangle + e^{i\frac{7\pi}{4}}|5\rangle + e^{i\frac{7\pi}{4}}|6\rangle + e^{i\frac{5\pi}{4}}|7\rangle + \\ + e^{i\frac{7\pi}{4}}|8\rangle + e^{i\frac{\pi}{4}}|9\rangle + e^{i\frac{\pi}{4}}|10\rangle + e^{i\frac{7\pi}{4}}|11\rangle + e^{i\frac{\pi}{4}}|12\rangle + e^{i\frac{7\pi}{4}}|13\rangle + e^{i\frac{7\pi}{4}}|14\rangle + e^{i\frac{\pi}{4}}|15\rangle\Big).$$

Analogamente, si ha che

$$|\tilde{\psi}_-^y\rangle = \frac{1}{4}\Big(e^{i\frac{\pi}{4}}|0\rangle + e^{i\frac{3\pi}{4}}|1\rangle + e^{i\frac{3\pi}{4}}|2\rangle + e^{i\frac{\pi}{4}}|3\rangle + e^{i\frac{3\pi}{4}}|4\rangle + e^{i\frac{\pi}{4}}|5\rangle + e^{i\frac{\pi}{4}}|6\rangle + e^{i\frac{3\pi}{4}}|7\rangle + \\ + e^{i\frac{5\pi}{4}}|8\rangle + e^{i\frac{3\pi}{4}}|9\rangle + e^{i\frac{3\pi}{4}}|10\rangle + e^{i\frac{5\pi}{4}}|11\rangle + e^{i\frac{3\pi}{4}}|12\rangle + e^{i\frac{5\pi}{4}}|13\rangle + e^{i\frac{5\pi}{4}}|14\rangle + e^{i\frac{3\pi}{4}}|15\rangle\Big).$$

A questo punto, si procede sostituendo nella (4.16) le espressioni ottenute per $|\tilde{\psi}_\pm^{x,y}\rangle$. Notando che, posto $\Xi^z = \sigma_1^z\sigma_2^z\sigma_3^z\sigma_4^z$, l'azione di tale operatore su ciascuno stato di base consiste nel moltiplicarlo per ± 1 a seconda che lo stato contenga o meno un numero dispari di 1 e considerando l'ortonormalità della base computazionale, si ottiene che

$$\langle\Sigma^x\rangle = 2\omega - 1, \quad \langle\Sigma^y\rangle = 0.$$

Anche in questo caso i calcoli completi sono riportati nell'appendice.

Sostituendo i valori medi nella (4.3), si ottiene la dipendenza funzionale che si stava cercando:

$$E(\rho_{exp}) = E(\omega) = \frac{1}{2}\Big(1 - 2\sqrt{\omega(1-\omega)}\Big). \tag{5.4}$$

5.2 Interagire con un computer quantistico: Qiskit

Per la parte sperimentale, ho adoperato il computer quantistico `ibmq_santiago`, uno dei dispositivi accessibili attraverso la piattaforma cloud IBM Quantum Experience, sviluppata dall'IBM Research [21].

A livello di hardware, i dispositivi IBM Quantum Experience sono basati su circuiti superconduttivi e giunzioni di Josephson. La Fig.5.1 mostra lo schema della struttura tipica di un chip quantistico a qubit superconduttivi, assieme all'impianto di raffreddamento.

I qubit superconduttivi, a differenza delle altre tipologie di qubit, non sono basati su entità microscopiche quali elettroni, ioni e fotoni. Sono basati su oscillatori elettrici (LC) e sono sistemi macroscopici con un elevato numero di atomi, solitamente di alluminio, assemblati in forma di fili metallici e piastre [15].

Le manipolazioni e le misurazioni sullo stato dei qubit avvengono mediante degli impulsi a microonde. Questi impulsi, inviati attraverso una linea di trasmissione accoppiata al qubit da manipolare, devono avere la stessa frequenza angolare di risonanza ω_{01} associata alla separazione energetica tra i due livelli del qubit (vedi Fig.5.2).
Per implementare gate a 2 qubit si rende necessario accoppiare i singoli qubit superconduttivi. Questo si realizza principalmente mediante accoppiamento capacitativo tra il campo di dipolo dei qubit e un risonatore (o una linea di alimentazione). In Fig.5.3 sono mostrati alcuni circuiti di accoppiamento capacitivo.

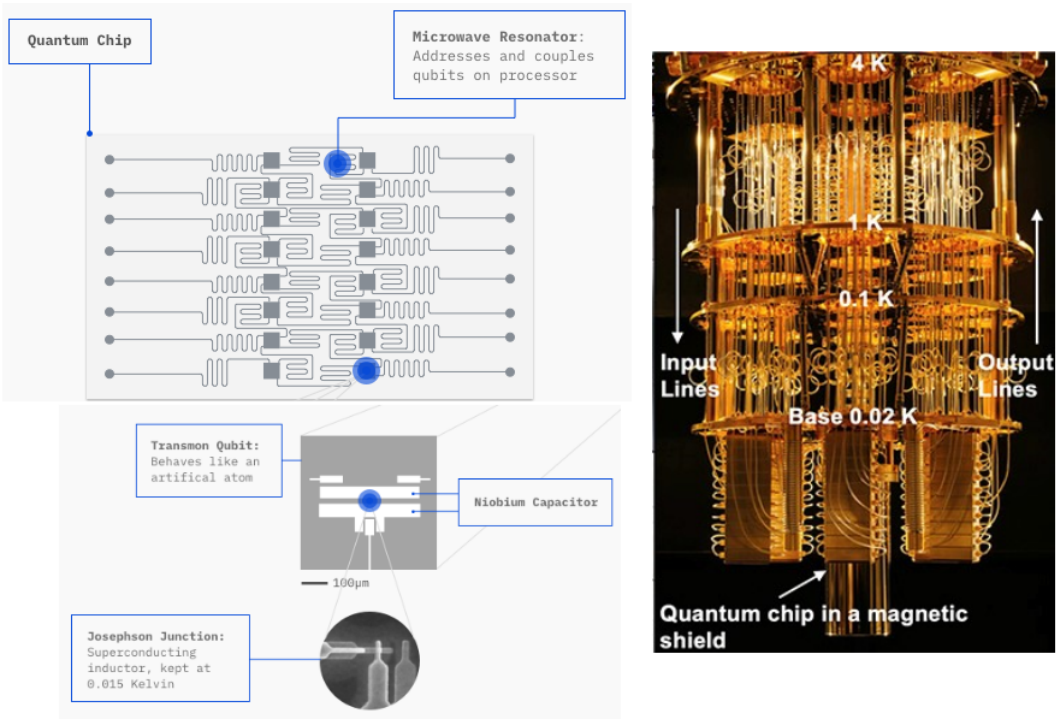


Figura 5.1: A sinistra è riportato lo schema di un chip quantistico a *transmon qubit* (Transmission line shunted plasma oscillation qubit): questo tipo di qubit viene realizzato attraverso un circuito LC con giunzione di Josephson. A destra è mostrata una foto di dispositivo completo IBM: chip quantistico e apparato di raffreddamento (4 diverse temperature di lavoro: 4 K, 1 K, 0.1 K e 0.02 K alla base). Fonte: IBM Quantum [21].

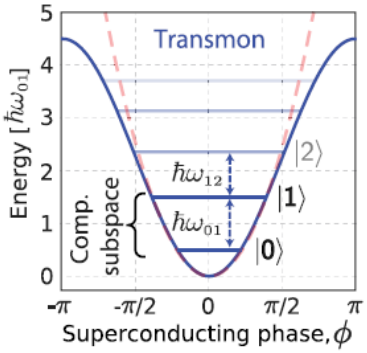


Figura 5.2: Schema di un circuito LC superconduttivo con giunzione di Josephson, il cui effetto è di produrre livelli energetici non equispaziati. Fonte: P. Krantz et al., 2019 [15].

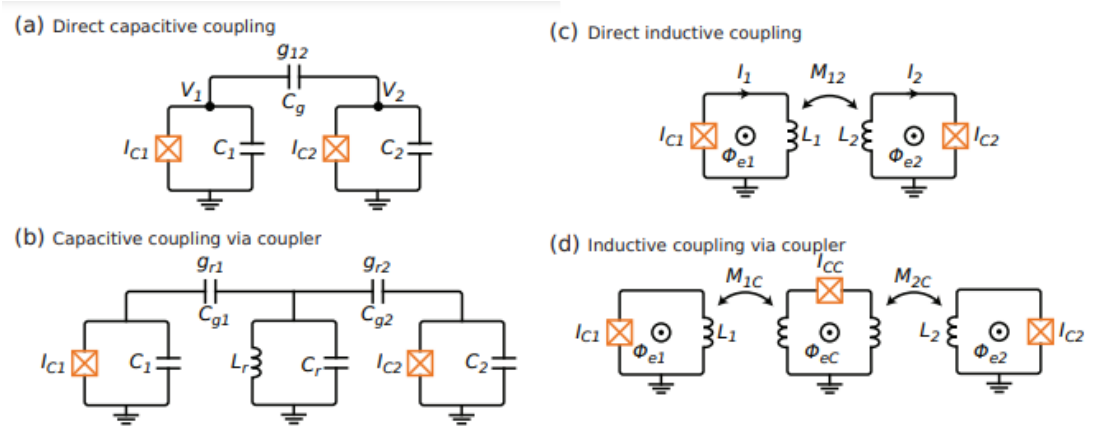


Figura 5.3: Schemi di possibili circuiti per realizzare l'accoppiamento di qubit superconduttivi. Fonte: P. Krantz et al., 2019 [15].

Interfacciarsi con questo tipo di hardware è chiaramente molto complesso e necessita di computazione sia classica sia quantistica.
A tal proposito, la IBM Research ha sviluppato Qiskit[1], un SDK (Software Development Kit) open source che copre tutti i passaggi che vanno dalla scrittura di algoritmi alla loro traduzione in codice eseguibile e quindi all'implementazione vera e propria sull'hardware, fino alla visualizzazione dei risultati della computazione.

Qiskit è a sua volta diviso in 4 sottogruppi, ordinati in librerie, i cui nomi si ispirano agli elementi naturali:

- Qiskit Terra → copre tutte le funzionalità a basso livello di Qiskit, che comprendono ad esempio la creazione e la manipolazione dei circuiti quantistici attraverso il linguaggio OpenQASM[2] o direttamente in Python.[3] Mette a disposizione anche una serie di funzioni per ottimizzare i circuiti nel momento in cui vengono adattati all'architettura di uno specifico computer quantistico, oltre a strumenti per modellare il rumore dei dispositivi fisici, fondamentale al fine di poter valutare gli esiti di una computazione. Infine, Terra comprende anche tutte le strutture necessarie all'organizzazione, lo storage e la manipolazione dei dati su cui poi intervengono le altre librerie;

- Qiskit Aqua → per trattare algoritmi quantistici ad alto livello. Riguarda soprattutto le applicazioni che non richiedono una conoscenza al dettaglio, da parte dell'utente, sulla costruzione dei circuiti quantistici, come ad esempio le applicazioni finanziarie, che spesso richiedono algoritmi molto complessi che poggiano anche su machine learning e procedure di ottimizzazione;

- Qiskit Aer → include un set di emulatori e simulatori per far girare i circuiti quantistici su macchine convenzionali. Risulta particolarmente utile nel momento in cui si

[1] Al momento sulla piattaforma è disponibile la versione 0.29.0, ma è stata recentemente rilasciata la 0.30.0 (vedi https://github.com/Qiskit/qiskit/releases).

[2] Si tratta di un linguaggio testuale sviluppato dall'IBM appositamente per fungere da intermediario tra l'utente e la fase di compilazione in linguaggio macchina. Ha elementi di C e di linguaggio assembly [6].

[3] La piattaforma IBM Quantum permette di redarre codice in forma di Jupyter Notebook e quindi la programmazione avviene principalmente in Python.

vogliono valutare i circuiti prima dell'esecuzione vera e propria sul computer quantistico, ad esempio per verificare che in assenza di rumore producano dei risultati attesi o per effettuare una stima degli effetti dovuti al rumore, riproducibile ad esempio tramite un modello;

- Qiskit Ignis → specifica per effettuare quantum error correction e caratterizzazione del rumore.

Le librerie Aqua e Ignis vengono utilizzate in applicazioni più avanzate rispetto ai circuiti richiesti dal protocollo di Kuzmak e Tkachuk. Illustrerò dunque solo alcune funzioni di base di Qiskit, in modo da dare un'idea generale delle sue caratteristiche.

Consideriamo come esempio un sistema a due qubit. Immaginiamo di volerlo preparare nello stato $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ su computer quantistico.
Dalla (3.3) sappiamo che per ottenere tale stato è necessario utilizzare prima un Hadamard gate e poi un CNOT gate. Riporto di seguito un semplice codice che effettua questa operazione:

```
1  from qiskit import QuantumRegister, ClassicalRegister, QuantumCircuit
2  from numpy import pi
3
4  qreg_q = QuantumRegister(2, 'q')
5  creg_c = ClassicalRegister(2, 'c')
6  circuit = QuantumCircuit(qreg_q, creg_c)
7
8  circuit.reset(qreg_q[0])
9  circuit.reset(qreg_q[1])
10 circuit.h(qreg_q[0])
11 circuit.cx(qreg_q[0], qreg_q[1])
```

La riga 1 serve ad importare le classi di Qiskit necessarie ad istanziare 3 tipi di oggetti (righe 4, 5, 6): un `QuantumRegister`, contente tutte le variabili necessarie a caratterizzare i 2 qubit da cui è composto il sistema; un `ClassicalRegister`, dove memorizzare gli esiti di eventuali misurazioni dei qubit (si ricorda infatti che un qubit, dopo essere stato misurato, equivale ad un bit classico); un `QuantumCircuit`, costruito a partire dai due registri e racchiudente i metodi necessari ad accedere e modificare i valori associati allo stato dei qubit, nonché ad implementare su di essi i gate quantistici.
Le righe 8, 9, 10 e 11 mostrano alcuni esempi di questi metodi: `reset` riporta il qubit che ha per argomento allo stato $|0\rangle$, mentre `h` applica un hadamard gate al qubit memorizzato in `qreq_q[0]` e `cx` effettua poi una trasformazione CNOT con `qreq_q[0]` come qubit di controllo e `qreq_q[1]` come qubit bersaglio.

Immaginiamo di voler verificare di aver ottenuto effettivamente il circuito atteso.
Un buon metodo è quello di aggiungere delle operazioni di misura al circuito e farlo poi girare su un backend, che può essere ad esempio un simulatore o un dispositivo reale. Vediamo intanto come occorre modificare il codice per adattarlo a questo tipo di compito, lasciando per ora in secondo piano la questione del backend. Il codice modificato è mostrato di seguito.

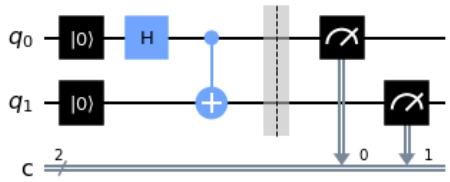
```
1  import numpy as np
2
3  # Importing standard Qiskit libraries
4  from qiskit import QuantumCircuit, transpile, Aer, IBMQ, QuantumRegister, ClassicalRegister, execute
5  from qiskit.providers.ibmq.managed import IBMQJobManager
6  from qiskit.tools.jupyter import *
7  from qiskit.visualization import *
8  from ibm_quantum_widgets import *
9  from qiskit.providers.aer import QasmSimulator
10
11 # Loading your IBM Quantum account(s)
12 provider = IBMQ.load_account()
13
14 qreg_q = QuantumRegister(2, 'q')
15 creg_c = ClassicalRegister(2, 'c')
16 circuit = QuantumCircuit(qreg_q, creg_c)
17
```

```
18 circuit.reset(qreg_q[0])
19 circuit.reset(qreg_q[1])
20 circuit.h(qreg_q[0])
21 circuit.cx(qreg_q[0], qreg_q[1])
22 circuit.barrier()
23 circuit.measure(qreg_q[0], creg_c[0])
24 circuit.measure(qreg_q[1], creg_c[1])
25
```

La funzione della riga 12, come recita il commento, serve semplicemente a caricare l'account IBM dell'utente, così da permettere al sistema di riconoscere a quali tipi di sistemi fisici può accedere.
Le righe 23, 24 aggiungono alla fine del circuito due operazioni di misura, che proiettano lo stato del qubit che ricevono per argomento in uno degli autostati $|0\rangle, |1\rangle$ dell'operatore di Pauli σ^z e salvano l'esito della misurazione nel ClassicRegister. Il comando `barrier` (riga 22) serve a mantenere separate, in fase di compilazione, le operazioni di misura da quelle di manipolazione.

A questo punto può essere utile una visualizzazione grafica del circuito. Ciò è realizzabile attraverso il metodo `draw`:

```
26 circuit.draw()
```



Ora, appurato che il circuito corrisponde a quanto si voleva realizzare, verifichiamone il corretto funzionamento prima con un simulatore e poi su un vero computer quantistico. Consideriamo prima il caso del simulatore.

```
28 # Use Aer's qasm_simulator
29 backend_sim = Aer.get_backend('qasm_simulator')
30 # Execute the circuit on the qasm simulator.
31 job = execute(circuit, backend_sim, shots=8192)
32
```

Il simulatore che ho scelto per questo esempio è `qasm_simulator` e appartiene alla libreria Aer, motivo per cui per essere selezionato necessita del comando `Aer.get_backend` (riga 29).
L'esecuzione del circuito sul simulatore avviene alla riga 31, con il comando `execute`. Questo comando deve ricevere obbligatoriamente almeno 2 argomenti: un oggetto (o una lista di oggetti) di tipo QuantumCircuit e un oggetto di tipo Backend o BaseBackend. Nell'esempio, questi requisiti sono soddisfatti da `circuit` e `backend_sim`. Il terzo argomento, `shots`, indica il numero di volte che il circuito deve essere eseguito sul backend. Come già accennato, lo scopo di questi programmi è ricostruire la probabilità di ottenere ciascuno stato di base in seguito ad una esecuzione del circuito, perciò la stima di tali probabilità avviene facendo girare n volte il circuito sul backend e andando a conteggiare quante volte viene ottenuto ciascuno stato di base.
Il numero massimo di shots impostabile rientra nelle specifiche dei backend, e nel caso del `qasm_simulator` è 8192.
Tra le specifiche troviamo inoltre anche il numero di qubit da cui è composto il sistema e il numero massimo di circuiti ad esso sottoponibili contemporaneamente.

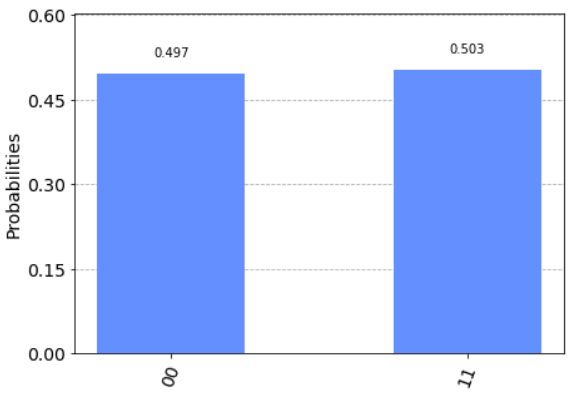
Il comando `execute` contiene al suo interno anche il processo di compilazione in linguaggio macchina, perciò non occorre l'intervento, almeno per il simulatore, di ulteriori funzioni.

Una volta terminata la computazione, è possibile recuperarne gli esiti con i seguenti comandi:

```
33 # Grab the results from the job.
34 result_job = job.result()
35 counts = result_job.get_counts(circuit)
36 print(counts)
37 plot_histogram(counts)
```

`job.result` restituisce un oggetto contente tutte le variabili relative alla computazione e in particolare è possibile estrarre, in forma di lista, le occorrenze di ciascuno stato di base tramite `get_counts`. Tale lista è di seguito stampata sia semplicemente nei suoi elementi, sia in forma di istogramma. Si noti che il numero di occorrenze viene automaticamente diviso per il numero di shots.

```
{'00': 4071, '11': 4121}
```



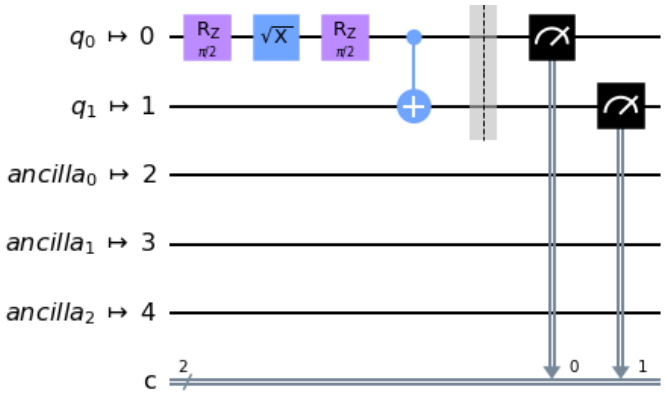
Se si vuole utilizzare come backend un dispositivo quantistico reale, occorre apportare al precedente codice due modifiche: cambiare il backend e aggiungere una chiamata della funzione `transpile`, che adatta il circuito (ottimizzandolo) all'architettura del backend.

```
28 # Use ibmq_santiago
29 backend_sim = provider.get_backend('ibmq_santiago')
30 circuit= transpile(circuit, backend=backend_sim)
```

Infatti, per un backend reale non tutti i gate sono direttamente disponibili: esiste solo un set universale di gate a partire dai quali vengono poi realizzati tutti gli altri gate. Nel caso di `ibmq_santiago`, il set universale comprende l'identità, il CNOT, RZ, $\sqrt{\text{X}}$ e X, dove

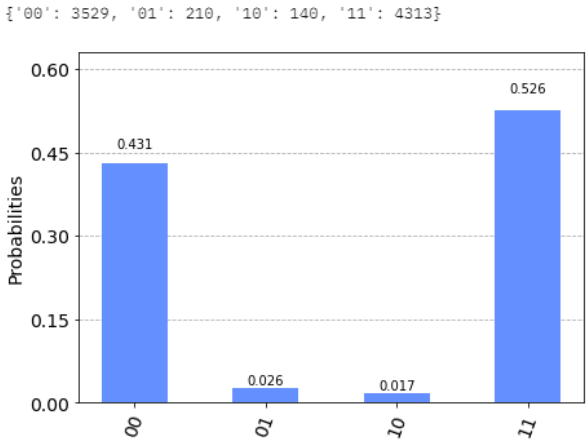
$$RZ(\lambda) = \exp\left(-i\frac{\lambda}{2}\sigma^z\right) = \begin{pmatrix} e^{-i\frac{\lambda}{2}} & 0 \\ 0 & e^{+i\frac{\lambda}{2}} \end{pmatrix}, \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sqrt{X} = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix},$$

nella loro forma matriciale.
Riporto di seguito l'aspetto del circuito dopo l'azione di `transpile`:



Notare che nel circuito sono riportati tutti i qubit disponibili sul dispositivo (5 in questo caso), anche quelli che non vengono alterati nel loro stato dal circuito.

Facendo girare il programma, si ottengono i seguenti risultati.



Dal confronto tra i risultati ottenuti con `qasm_simulator` e quelli ottenuti con `ibmq_santiago` si possono mettere in luce alcune importanti considerazioni:

- l'esito della computazione eseguita sul simulatore si avvicina moltissimo al risultato atteso, ovvero circa un 50% di stato $|00\rangle$ e un 50% di $|11\rangle$. Un risultato ancora più preciso si potrebbe raggiungere se fosse possibile aumentare ulteriormente il numero di shots;
- nel caso del dispositivo reale, si possono notare gli effetti del rumore. È presente infatti un numero non trascurabile di occorrenze degli stati $|01\rangle$ e $|10\rangle$. Ciò è dovuto al fatto che `ibmq_santiago` è formato da qubit reali, che possono essere soggetti a perturbazioni, e i suoi gate sono impulsi elettromagnetici e quindi anch'essi soggetti ad errore. Nella prossima sezione tornerò poi su questo aspetto.

Questo esempio di applicazione di Qiskit racchiude al suo interno tutte le funzioni che ho utilizzato nel programma da me redatto per implementare il protocollo di Kuzmak e Tkachuk. Nella prossima sezione dunque mi concentrerò principalmente sui circuiti e su come ho strutturato le loro esecuzioni, piuttosto che sul codice.

5.3 L'entanglement stimato con ibmq_santiago

Per calcolare l'entanglement del primo qubit rispetto al resto di un sistema a 4 qubit, sappiamo che per lo stato (5.1) è necessario valutare 4 valori medi:

$$\langle\psi_+|\Sigma^x|\psi_+\rangle\,, \quad \langle\psi_-|\Sigma^x|\psi_-\rangle\,, \quad \langle\psi_+|\Sigma^y|\psi_+\rangle\,, \quad \langle\psi_-|\Sigma^y|\psi_-\rangle\,. \tag{5.5}$$

Tali valori medi sono ricavabili facilmente una volta calcolati gli stati (5.3). Ciascun valore medio è infatti dato dalla somma delle probabilità di trovare, in seguito ad una misurazione dello stato $|\tilde{\psi}^{x,y}_{\pm}\rangle$ in cui è stato preparato il sistema, ciascuno stato della base computazionale, moltiplicando opportunamente tali probabilità per ± 1 secondo le relazioni (A.1).

Per applicare il protocollo di Kuzmak e Tkachuk, ho dunque costruito in Qiskit quattro circuiti, uno per ogni valor medio, volti a manipolare lo stato $|0000\rangle$ fino ad ottenere $|\tilde{\psi}^{x,y}_{\pm}\rangle$. Facendoli girare su un backend (prima un simulatore e poi un dispositivo reale) ho quindi determinato le ampiezze associate a ciascuno stato di base, in modo da ricostruire la composizione in termini di stati di base di $|\tilde{\psi}^{x,y}_{\pm}\rangle$.
I circuiti, che si rifanno allo schema generale in Fig.4.3, sono riportati nella prossima pagina nella loro struttura a blocchi.
Si noti che nei circuiti è stato necessario impostare un angolo di $-\pi/2$ per il gate RY. Infatti, sia RX che RY sono nella forma

$$RX(\theta) = \exp\left(-i\frac{\theta}{2}\sigma^x\right) = \begin{pmatrix} \cos(\theta/2) & -i\sin(\theta/2) \\ -i\sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$$
$$RY(\theta) = \exp\left(-i\frac{\theta}{2}\sigma^y\right) = \begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}.$$

Per la parte relativa alla simulazione, ho utilizzato come backend `qasm_simulator`. Per riprodurre l'ensemble associato allo stato misto, ho introdotto una variabile N con valore 8192 (il massimo numero di shots per circuito effettuabili da `qasm_simulator`) e poi ho impostato per i circuiti associati a $|\tilde{\psi}^k_+\rangle$, $k = x, y$, un numero di shots pari a ωN, mentre per quelli associati a $|\tilde{\psi}^k_-\rangle$ ho impostato $(1-\omega)N$ shots. Così facendo, si ha che in assenza di misurazione i circuiti riproducono un insieme di N stati formato da $N\omega$ copie dello stato $|\tilde{\psi}^k_+\rangle$ e $N(\omega-1)$ copie dello stato $|\tilde{\psi}^k_-\rangle$, che è esattamente l'ensemble associato allo stato misto (5.1).

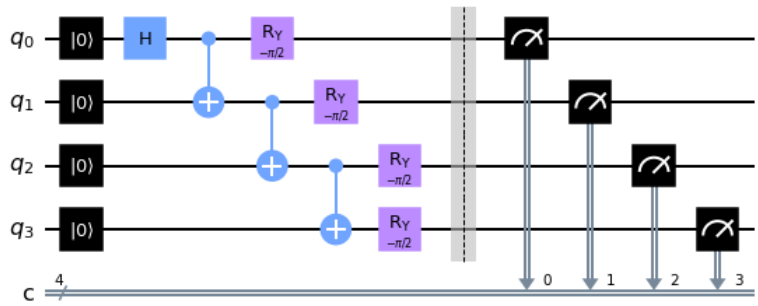


Figura 5.4: Circuito relativo a $|\tilde{\psi}^x_+\rangle$.

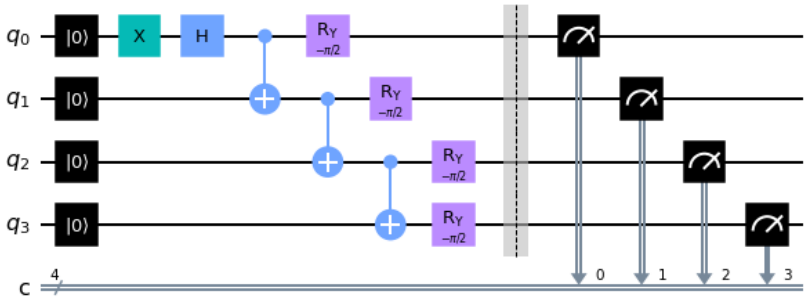


Figura 5.5: Circuito relativo a $|\tilde{\psi}^x_-\rangle$.

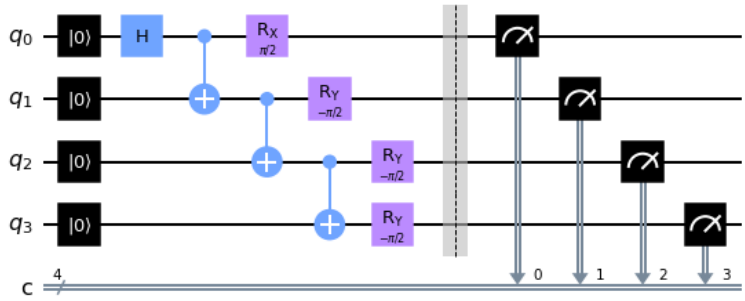


Figura 5.6: Circuito relativo a $|\tilde{\psi}^y_+\rangle$.

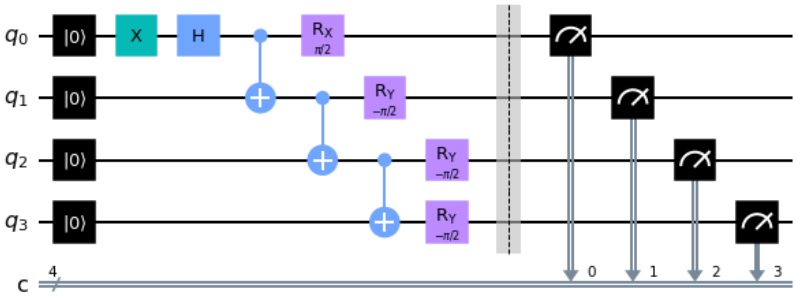


Figura 5.7: Circuito relativo a $|\tilde{\psi}^y_-\rangle$.

Come risultato della computazione, ho ottenuto quattro distribuzioni di probabilità degli stati della base computazionale, una per ogni stato $|\tilde{\psi}_{\pm}^{x,y}\rangle$.
A partire da esse, ho calcolato ciascun valor medio esattamente come nel caso analitico, ovvero andando a moltiplicare ciascuna probabilità per ± 1 a seconda dello stato corrispondente e poi sommandole.
Per ottenere $\langle\Sigma^x\rangle$ e $\langle\Sigma^y\rangle$ ho combinato i valori medi (5.5) secondo i pesi ω e $1-\omega$ (vedi equazioni (5.2)). Infine, ho calcolato l'entanglement sostituendo $\langle\Sigma^x\rangle$ e $\langle\Sigma^y\rangle$ nella (4.3).

Per ottenere l'andamento dell'entanglement in funzione di ω, ho ripetuto il procedimento appena descritto 19 volte, facendo variare ω come riportato in tabella 5.1. Ovviamente ho impostato valori di ω tali per cui sia $N\omega$ sia $N(1-\omega)$ risultassero numeri interi, dato che il numero di shots deve essere un intero.

ω	$E(\rho_{exp})$	ω	$E(\rho_{exp})$
0.984375	0.3759804072938473	0.4375	0.003950706731751574
0.96875	0.3260073636615617	0.375	0.015932488365825004
0.9375	0.2579445737596325	0.3125	0.03649685337513364
0.875	0.16930003307614927	0.25	0.06700383375358537
0.8125	0.10969451620453874	0.1875	0.10976100920542181
0.75	0.0670027841256649	0.125	0.16930003307614927
0.6875	0.03651204402506403	0.0625	0.2579386639808925
0.625	0.015882068062157806	0.03125	0.3260073636615618
0.5625	0.003960695025349015	0.015625	0.3759804072938473
0.5	0.00013734796602626886		

Tabella 5.1: Risultati della simulazione su `qasm_simulator`. I valori di entaglement ottenuti sono riportati assieme al parametro ω impostato.

I valori $\omega = 0$ e $\omega = 1$ non compaiono nella tabella. Sono stata costretta ad escluderli perché ho osservato che per tali valori le fluttuazioni sulle probabilità, che come si è visto nella scorsa sezione non sono fonte di rumore quanto piuttosto di un numero non sufficientemente alto di shots, causavano una combinazione di $\langle\Sigma^x\rangle$, $\langle\Sigma^y\rangle$ per cui l'entanglement risultava un numero immaginario, anziché tendente a 0.5 come ci si aspetterebbe dalla (5.4).

Per quanto riguarda l'esperimento su dispositivo reale, ho selezionato come backend `ibmq_santiago`, la cui architettura è mostrata nella Fig.5.8.
Per calcolare l'entanglement ho seguito lo stesso procedimento descritto nella simulazione, lasciando N impostato a 8192. Ho dovuto aggiungere però quattro chiamate di `transpile`, una per ogni circuito, in modo da adattarli e ottimizzarli alla struttura di `ibmq_santiago`. Riporto nelle Fig.5.9, 5.10, 5.11, 5.12 i circuiti nella loro versione transpiled.

In questo caso conoscere la forma dei circuiti adattata a `ibmq_santiago` è fondamentale, perché permette di valutare se il circuito è in grado di fornire risultati attendibili e, in caso affermativo, di fare una stima dell'errore associato a ciascun valore di $E(\rho_{exp})$ ottenuto.
Un computer quantistico reale, infatti, è soggetto a fenomeni di rilassamento e dephasing, che dopo un certo intervallo di tempo possono produrre effetti tali da invalidare i risultati della computazione.

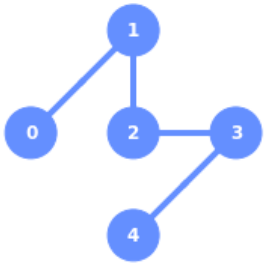


Figura 5.8: Schema dell'architettura di `ibmq_santiago`.

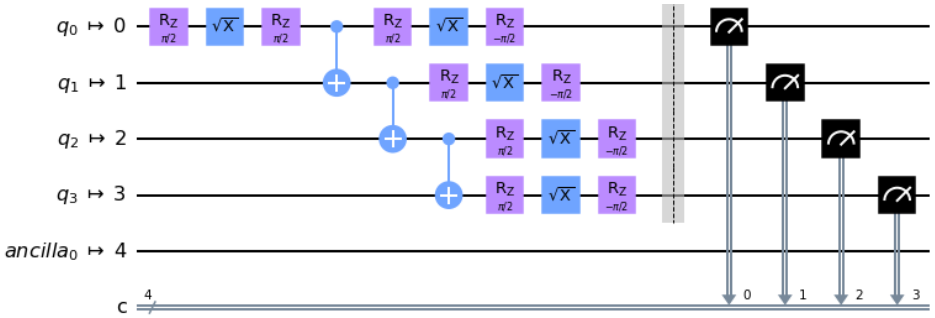


Figura 5.9: Versione transpiled del circuito di $|\tilde{\psi}^x_+\rangle$.

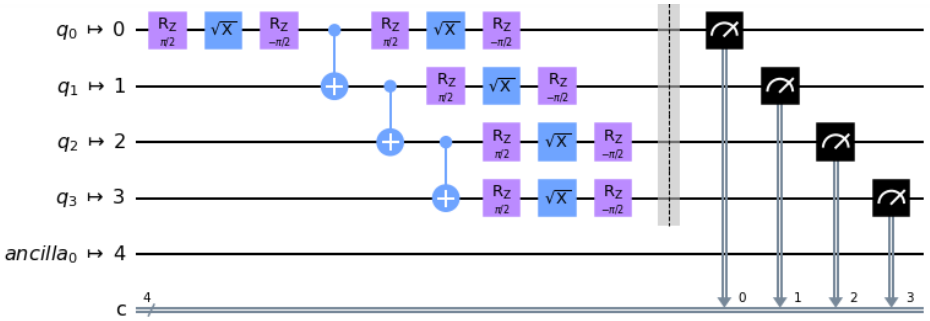


Figura 5.10: Versione transpiled del circuito di $|\tilde{\psi}^x_-\rangle$.

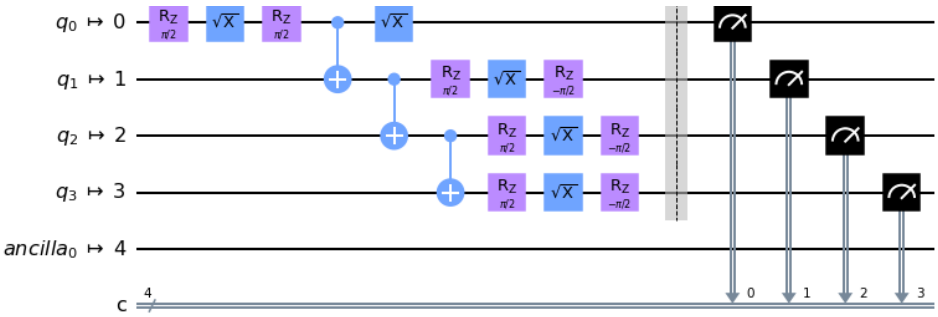


Figura 5.11: Versione transpiled del circuito di $|\tilde{\psi}^y_+\rangle$.

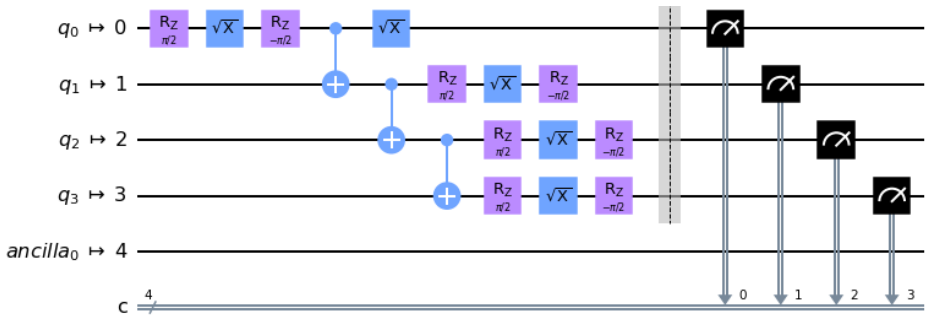


Figura 5.12: Versione transpiled del circuito di $|\tilde{\psi}^y_-\rangle$.

Dato che ciascun gate necessita di un certo tempo per essere applicato ai qubit, è importante controllare che il tempo complessivo non ecceda quello di attendibilità della misura.

I dati necessari a questo tipo di valutazione sono estrapolabili dai dati di calibrazione del computer quantistico, costantemente aggiornati e scaricabili da [21] nell'apposita sezione dedicata ai sistemi quantistici.
Nella tabella 5.2 ho riportato i dati di calibrazione di `ibmq_santiago` risalenti al giorno e all'orario in cui ho effettuato l'acquisizione dati (11.08.2021, ore 21.45 circa).

Qubit	T_1(µs)	T_2(µs)	Frequenza (GHz)	Readout error (10^{-2})	Single-qubit gate error (10^{-4})	CNOT error (10^{-2}), gate time (ns)
Q_0	59.68	136.81	4.833	2.590	5.724	0_1: 1.360, 526.222
Q_1	55.94	92.65	4.624	4.040	4.080	1_2: 0.6777, 355.556
Q_2	92.19	74.34	4.821	1.000	1.918	2_3: 0.6815, 376.889
Q_3	97.83	74.36	4.742	0.8600	2.437	

Tabella 5.2: Dati di calibrazione di `ibmq_santiago` al momento dell'acquisizione dati. Sono riportati solo i dati relativi ai qubit impiegati nell'esperimento (Q_0, Q_1, Q_2, Q_3) e ai gate universali: CNOT e i 3 gate identità, X, $\sqrt{X}$ (non vi sono errori su RZ). Nel CNOT, la notazione A_B indica A qubit di controllo e B qubit bersaglio. T_1 e T_2 sono rispettivamente il tempo di rilassamento e il tempo di dephasing. *Frequenza* identifica la differenza energetica tra stato $|0\rangle$ e stato $|1\rangle$ di ogni qubit, *Readout error* l'errore di lettura.

I tempi T_1, T_2 riportati nella tabella 5.2 rappresentano rispettivamente l'intervallo di tempo dall'inizio di uno shot entro cui rilassamento e dephasing non inficiano i risultati. Un circuito, per fornire risultati attendibili, deve avere quindi un tempo di esecuzione inferiore al minimo tra i T_1 e T_2 dei 4 qubit.
Le operazioni che richiedono il maggior tempo sono i CNOT gate, perché prevedono un'accoppiamento di due qubit, quindi in questo caso il tempo medio necessario ad eseguire le operazioni CNOT di ciascun circuito è dato da:

$$T_{0\_1} + T_{1\_2} + T_{2\_3} = (526.222 + 355.556 + 376.889)\text{ns} = 1.258667\,\mu\text{s},$$

dove T_{A_B} indica il tempo necessario affinché il qubit A, che funge da controllo, venga accoppiato al qubit bersaglio B e agisca su di esso.
Gli ulteriori gate che compaiono nel circuito sono i gate $\sqrt{X}$ e RZ. RZ è istantaneo, mentre $\sqrt{X}$ ha un tempo di esecuzione[4] di 35.55 ns, un ordine di grandezza inferiore rispetto al CNOT.
Il tempo complessivo di esecuzione del circuito è quindi indubbiamente molto inferiore al minimo tra T_1 e T_2 (55.94 µs).

Chiarito quindi che il circuito è a priori in grado di fornire risultati attendibili, vediamo come quantificare gli errori connessi a tali risultati.

Per associare un errore a ciascun valor medio calcolato, ho ragionato nel seguente modo. Ad ogni shot, il computer quantistico restituisce uno stato misurato. Le fonti di errore su tale stato sono:

- errori di lettura (*readout error*);
- errori nell'esecuzione dei vari gate (*gate error*);

I gate error sono facilmente quantificabili, nel caso presente: i gate RZ infatti oltre ad essere istantanei sono anche infallibili[5], perciò le uniche fonti di errore nei 4 circuiti sono i 3 CNOT gate e i 5 $\sqrt{X}$. Detto Δ_{gate} l'errore relativo dovuto ai gate error, ho quindi che per tutti e 4 i circuiti

$$\Delta_{gate} = 2\Delta^0_{\sqrt{X}} + \Delta^1_{\sqrt{X}} + \Delta^2_{\sqrt{X}} + \Delta^3_{\sqrt{X}} + \Delta^{0\_1}_{CNOT} + \Delta^{1\_2}_{CNOT} + \Delta^{2\_3}_{CNOT},$$

dove i pedici indicano il tipo di gate e gli apici i qubit a cui corrispondono i vari errori. Sostituendo i dati della tabella 5.2, si ottiene che

$$\begin{aligned}\Delta_{gate} &= 10^{-2} \cdot (2 \cdot 0.05724 + 0.04080 + 0.01918 + 0.02437 + 1.36 + 0.6777 + 0.6815) = \\ &= 0.0291804\end{aligned} \tag{5.6}$$

Gli errori di lettura invece si verificano quando il computer, terminata una misura sullo stato di un qubit, non riesce ad identificare correttamente l'esito della computazione.
Nei circuiti che si stanno considerando, ad ogni shot vengono consecutivamente misurati 4 qubit, mentre i readout error che appaiono nella tabella 5.2 sono frutto di stime fatte sui singoli qubit.
Una soluzione a questa problematica è proposta nell'appendice B di [1] e si articola come segue.
Tra i dati di calibrazione disponibili per `ibmq_santiago` vi sono anche le probabilità p_{01} e p_{10} che il computer attibuisca, in seguito a misurazione, rispettivamente valore 0 ad un qubit preparato nello stato $|1\rangle$ e valore 1 ad un qubit preparato in $|0\rangle$ (vedi tabella 5.3).

La probabilità dunque che lo stato $|0000\rangle$ venga identificato come tale è data da

$$F_0 = (1 - p^0_{10})(1 - p^1_{10})(1 - p^2_{10})(1 - p^3_{10}) = 0.9499,$$

mentre la probabilità che $|1111\rangle$ sia correttamente misurato è

$$F_1 = (1 - p^0_{01})(1 - p^1_{01})(1 - p^2_{01})(1 - p^3_{01}) = 0.8859.$$

Qubit	p_{01}	p_{10}
Q_0	0.0432	0.0086
Q_1	0.0492	0.0316
Q_2	0.014	0.006
Q_3	0.0126	0.0046

Tabella 5.3: Dati di calibrazione relativi alla probabilità p_{01}^k che il qubit k, preparato in $|1\rangle$, all'atto della misurazione venga valutato 0, mentre p_{10}^k è la probabilità che si verifichi il viceversa.

La probabilità media che uno stato venga correttamente letto è stimabile come

$$F = \frac{F_1 + F_2}{2},$$

perciò l'errore medio di lettura Δ_{lett} sarà

$$\Delta_{lett} = 1 - F = 0.0821. \tag{5.7}$$

L'errore relativo totale da applicare a ciascuno dei valori medi (5.5) è dunque pari a

$$\Delta = \Delta_{gate} + \Delta_{lett} = 0.1113. \tag{5.8}$$

Chiarita la gestione degli errori, riporto in forma grafica (Fig.5.13) un esempio di risultati forniti da `ibmq_santiago` relativamente allo stato $|\tilde{\psi}_+^x\rangle$ e a $|\tilde{\psi}_+^y\rangle$, con $\omega = 0.1875$.

Passiamo dunque ai risultati ottenuti con `ibmq_santiago`.
A differenza della simulazione, in questo caso l'entanglement è stato calcolato per 17 diversi valori di ω. Riporto i risultati ottenuti sia in forma di tabella (vedi tabella 5.4), sia in forma grafica (Fig.5.14).
Il grafico in Fig.5.14 mette direttamente a confronto l'andamento di $E(\rho_{exp})$ in funzione di ω ricavato sperimentalmente con quello simulato (i dati sono riportati nella tabella 5.1) e con quello ricavato analiticamente (relazione (5.4)). Il calcolo dettagliato degli errori è riportato in Appendice.

Da un'analisi combinata dei grafici in Fig.5.14 e 5.13, emerge chiaramente che il protocollo sperimentale proposto in [1] è in grado di riprodurre l'entanglement geometrico dello stato (5.1) ricavato analiticamente, dato che la simulazione ne ricalca perfettamente l'andamento. Tuttavia, a causa delle fluttuazioni nelle distribuzioni di probabilità, il dispositivo reale fornisce dei valori che riproducono a livello di forma l'andamento corretto, ma non sono sufficientemente accurati per valori di ω a cui corrispondono ensemble fortemente asimmetrici. Si può notare infatti come l'accordo dei dati con l'andamento analitico peggiori man mano che da $\omega = 0.5$ ci si sposta verso $\omega = 0$ e $\omega = 1$.

Questo comportamento è osservato anche in [1]. Nell'articolo, la causa di questa discrepanza viene addotta principalmente a due motivazioni:

[4] I tempi di esecuzione di ciascun gate sono forniti dalla funzione `properties` della classe `Backend`.

[5] Questi gate rappresentano rotazioni attorno all'asse z della sfera di Bloch, perciò non vengono realmente implementati: se ne tiene memoria tramite software e si realizza invece una rotazione degli assi x e y, che si traduce in un update dell'azione dei gate X e Y.

- l'errore di lettura diventa sempre più consistente a mano a mano che aumenta il numero di qubit da misurare; questo primo punto è supportato dal fatto che i risultati riportati in [1] si avvicinano molto di più all'andamento teorico quando l'analisi viene effettuata su un sistema a due qubit piuttosto che a 4 qubit;

- nel caso $\omega = 0.5$, l'operatore di densità assume la forma massimamente mista $\rho_{exp} = \frac{1}{2}(|0000\rangle\langle 0000| + |1111\rangle\langle 1111|)$. Tale operatore di densità rappresenta uno stato misto non entangled (gli stati puri che costituiscono l'ensemble sono separabili) ed i suoi autostati fanno parte degli stessi stati che compongono la base in cui avviene la misurazione. Di conseguenza, sembra che la misurazione sia più accurata per gli stati misti che più si avvicinano a questo particolare ρ_{exp}.

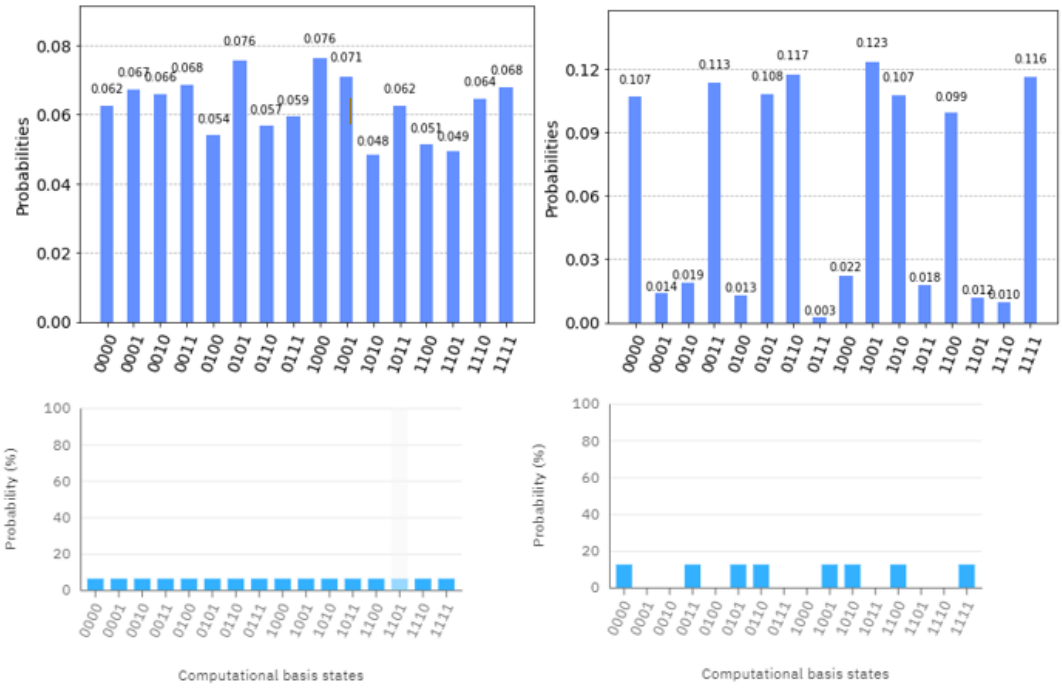


Figura 5.13: In alto: a sinistra distribuzione delle probabilità di ottenere ciascuno stato di base preparando $|0000\rangle$ in $|\tilde{\psi}^y_+\rangle$, a destra distribuzione relativa a $|\tilde{\psi}^x_+\rangle$ (risultati ottenuti con `ibmq_santiago`, $\omega = 0.1875$). In basso: distribuzioni ideali riprodotte con Quantum Composer, un'interfaccia grafica disponibile su IBM Quantum Experience per creare e testare circuiti senza scrivere esplicitamente alcun codice.

ω	$E(\rho_{exp}) \pm \Delta E$	ω	$E(\rho_{exp}) \pm \Delta E$
1	0.19 ± 0.05	0.4375	0.003 ± 0.003
0.9375	0.14 ± 0.04	0.375	0.010 ± 0.006
0.875	0.09 ± 0.03	0.3125	0.02 ± 0.01
0.8125	0.07 ± 0.02	0.25	0.04 ± 0.01
0.75	0.05 ± 0.02	0.1875	0.07 ± 0.02
0.6875	0.018 ± 0.009	0.125	0.10 ± 0.03
0.625	0.010 ± 0.007	0.0625	0.14 ± 0.04
0.5625	0.003 ± 0.003	0	0.20 ± 0.06
0.5	0.0001 ± 0.0001		

Tabella 5.4: Risultati ottenuti con `ibmq_santiago`. I valori di entaglement ottenuti sono riportati assieme al parametro ω impostato. Per la derivazione degli errori, si veda l'Appendice.

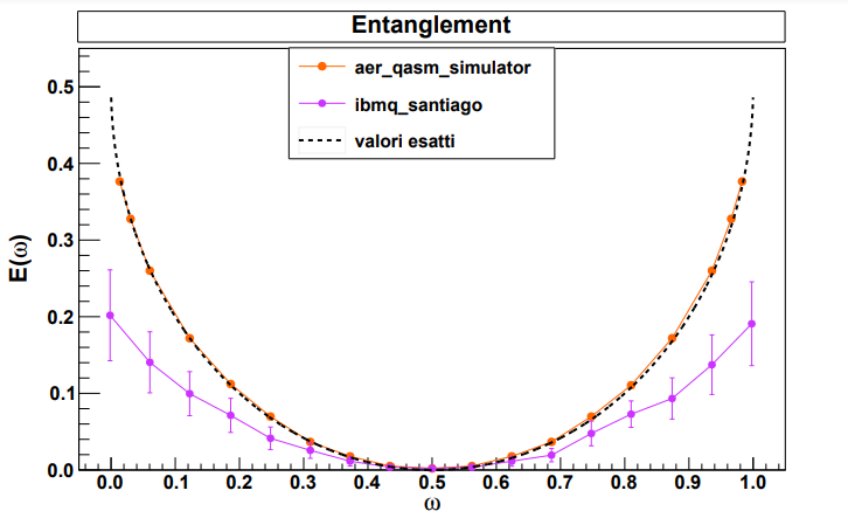


Figura 5.14: Grafico in cui vengono messi a confronto gli andamenti dell'entanglement in funzione di ω ricavati analiticamente (linea nera tratteggiata), tramite simulazione su `qasm_simulator` (marcatori arancioni collegati da linea continua) e sperimentalmente con `ibmq_santiago` (marcatori viola collegati da linea spezzata, barre di errore verticali anch'esse viola).

Conclusione

Nel caso dello stato misto del sistema a 4 qubit analizzato nella precedente sezione, il protocollo sperimentale proposto da Kuzmak e Tkachuk in [1] fornisce, nel caso della simulazione, dei risultati che ricalcano perfettamente il comportamento analitico atteso. Infatti, come messo in evidenza dalla Fig.5.14, variando la proporzione di stati $|\psi_+\rangle$ e $|\psi_-\rangle$ nell'ensemble dello stato misto, il valore ottenuto per l'entropia di entanglement del primo qubit rispetto agli altri 3 che compongono il sistema combacia con il valore che si ottiene sostituendo ciascun ω impostato nell'espressione $E(\omega) = \frac{1}{2}(1 - 2\sqrt{\omega(1-\omega)})$, ricavata applicando il protocollo analitico.

Nonostante gli ottimi risultati ottenuti con la simulazione, che evidenziano di fatto la correttezza di procedimento sperimentale e analitico, nel momento in cui si utilizza un dispositivo reale quale `ibmq_santiago` i risultati ottenuti non sono altrettanto soddisfacenti.
L'andamento dei valori dell'entanglement, per quanto sia simile a quello di $E(\omega)$, si discosta sempre più da quello atteso man mano che l'ensemble tende ad uno stato puro. Resta comunque interessante che il protocollo sperimentale sia in grado di identificare perfettamente uno stato non entangled: per $\omega = 0.5$, lo stato misto infatti diventa $\rho_{exp}^{max} = \frac{1}{2}(|0000\rangle\langle 0000| + |1111\rangle\langle 1111|)$, che corrisponde ad uno stato misto con ensemble composto da un 50% di stati $|0000\rangle$ e un 50% di $|1111\rangle$, che lo rendono uno stato misto separabile.

In [1], la discrepanza significativa tra dati sperimentali e valori attesi viene addotta a due fattori: alla dipendenza dell'errore di lettura dal numero di qubit misurato e alla distanza dello stato (5.1) dallo stato massimamente misto ρ_{exp}^{max}.
Il primo fattore è supportato dai risultati riportati nell'articolo, che sono molto più precisi quando ottenuti applicando il protocollo ad un sistema a 2 qubit nello stato $\rho = \omega\,|\Phi^+\rangle\langle\Phi^+| + (1-\omega)\,|\Phi^-\rangle\langle\Phi^-|$, con $\omega \in [0,1]$ e $|\Phi^+\rangle$, $|\Phi^-\rangle$ stati di Bell (vedi (3.2)), piuttosto che quelli ottenuti applicandolo a un sistema a 4 qubit nello stato (5.1).
Il secondo fattore invece discende dal fatto che gli autostati di ρ_{exp}^{max} coincidono con due degli stati della base in cui avviene la misurazione, perciò in tal caso la misurazione potrebbe effettivamente essere più accurata e meno soggetta ad errori. Ci si aspetterebbe dunque, in base a queste considerazioni, di riscontrare risultati più precisi attorno a $\omega = 0.5$ e di vederli peggiorare man mano che ci si allontana dallo stato separato e si va verso gli stati più entangled, e questo è esattamente ciò che si osserva.

In [1] questo aspetto viene approfondito sperimentalmente per un sistema a 2 qubit, ma sarebbe molto interessante analizzare anche il caso di un sistema a 4 qubit, per testare l'impatto dell'aumento del numero di qubit.

A mio avviso, sarebbe anche utile e auspicabile provare a testare il protocollo preparando sempre 4 qubit nello stato (5.1) ma su computer quantistici con architettura diversa,

ad esempio con connessioni tra i qubit non a catena. Così facendo si valuterebbe anche un eventuale ruolo della struttura del computer quantistico nell'accuratezza del protocollo.

Oltre a svolgere studi più approfonditi sull'origine della discrepanza tra comportamento atteso e risultati ottenuti tramite dispositivo reale, potrebbe essere interessante implementare delle operazioni di *measurement error mitigation*.
Si tratta di particolari procedure in cui viene quantificato l'effetto del rumore sulla misura di ciascuno stato della base computazionale. A partire dai dati ottenuti, si costruisce poi un modello degli effetti del rumore e lo si impiega come "filtro" dei dati sperimentali.
Qiskit offre strumenti appositi per questo tipo di analisi, contenuti principalmente in Qiskit Aer e Qiskit Ignis (si veda la sezione 5.2 di [3] per un esempio) e sarebbe molto interessante includerli nel protocollo sperimentale per testarne l'efficacia.
Una buona procedura di measurement error mitigation potrebbe addirittura risolvere alla radice il problema della sensibilità dei risultati dagli errori di lettura.

Appendice A

Calcolo analitico dell'entanglement geometrico di ρ_{exp}

$$
\begin{aligned}
|\tilde{\psi}^x_+\rangle &= \Big(\frac{1}{\sqrt{2}}\Big)^5 (I_1 + i\sigma^y_1)(I_2 + i\sigma^y_2)(I_3 + i\sigma^y_3)(I_4 + i\sigma^y_4)\Big(|0\rangle_1 |0\rangle_2 |0\rangle_3 |0\rangle_4 + |1\rangle_1 |1\rangle_2 |1\rangle_3 |1\rangle_4\Big) \\
&= \frac{1}{4\sqrt{2}}(I_1 + i\sigma^y_1)(I_2 + i\sigma^y_2)(I_3 + i\sigma^y_3)\Big(|0000\rangle - |0001\rangle + |1111\rangle + |1110\rangle\Big) \\
&= \frac{1}{4\sqrt{2}}(I_1 + i\sigma^y_1)(I_2 + i\sigma^y_2)\Big(|0000\rangle - |0001\rangle + |1111\rangle + |1110\rangle - |0010\rangle + \\
&+ |0011\rangle + |1101\rangle + |1100\rangle\Big) \\
&= \frac{1}{4\sqrt{2}}(I_1 + i\sigma^y_1)\Big(|0000\rangle - |0001\rangle + |1111\rangle + |1110\rangle - |0010\rangle + |0011\rangle + |1101\rangle + \\
&+ |1100\rangle - |0100\rangle + |0101\rangle + |1011\rangle + |1010\rangle + |0110\rangle - |0111\rangle + |1001\rangle + |1000\rangle\Big) \\
&= \frac{1}{4\sqrt{2}}\Big(|0000\rangle - \cancel{|0001\rangle} + |1111\rangle + \cancel{|1110\rangle} - \cancel{|0010\rangle} + |0011\rangle + \cancel{|1101\rangle} + |1100\rangle + \\
&- \cancel{|0100\rangle} + |0101\rangle + \cancel{|1011\rangle} + |1010\rangle + |0110\rangle - \cancel{|0111\rangle} + |1001\rangle + \cancel{|1000\rangle} - \cancel{|1000\rangle} + \\
&+ |1001\rangle + \cancel{|0111\rangle} + |0110\rangle + |1010\rangle - \cancel{|1011\rangle} + |0101\rangle + \cancel{|0100\rangle} + |1100\rangle - \cancel{|1101\rangle} + \\
&+ |0011\rangle + \cancel{|0010\rangle} - \cancel{|1110\rangle} + |1111\rangle + \cancel{|0001\rangle} + |0000\rangle\Big),
\end{aligned}
$$

da cui, esprimendo ciascuno stato di base in forma decimale,

$$
|\tilde{\psi}^x_+\rangle = \frac{1}{2\sqrt{2}}\Big(|0\rangle + |15\rangle + |3\rangle + |12\rangle + |5\rangle + |10\rangle + |6\rangle + |9\rangle\Big).
$$

Analogamente si ottiene che

$$
\begin{aligned}
|\tilde{\psi}^x_-\rangle &= \frac{-1}{2\sqrt{2}}\Big(|1000\rangle + |0100\rangle + |0010\rangle + |1110\rangle + |0001\rangle + |1101\rangle + |1011\rangle + |0111\rangle\Big) \\
&= \frac{-1}{2\sqrt{2}}\Big(|1\rangle + |2\rangle + |4\rangle + |7\rangle + |8\rangle + |11\rangle + |13\rangle + |14\rangle\Big).
\end{aligned}
$$

Per quanto riguarda $|\tilde{\psi}^y_+\rangle$, si ricorda che

$$
e^{-i\frac{\pi}{4}\sigma^x} = \cos\Big(-\frac{\pi}{4}\Big)I + i\sin\Big(-\frac{\pi}{4}\Big)\sigma^x = \frac{1}{\sqrt{2}}(I - i\sigma^x) = \frac{1}{\sqrt{2}}(I - i\,|0\rangle\langle 1| - i\,|1\rangle\langle 0|),
$$

quindi si ottiene che

$$
\begin{aligned}
|\tilde{\psi}^y_+\rangle &= \Big(\frac{1}{\sqrt{2}}\Big)^5 (I_1 - i\sigma^x_1)(I_2 + i\sigma^y_2)(I_3 + i\sigma^y_3)(I_4 + i\sigma^y_4)\Big(|0\rangle_1 |0\rangle_2 |0\rangle_3 |0\rangle_4 + |1\rangle_1 |1\rangle_2 |1\rangle_3 |1\rangle_4\Big) \\
&= \frac{1}{4\sqrt{2}}(I_1 - i\sigma^x_1)\Big(|0000\rangle - |0001\rangle + |1111\rangle + |1110\rangle - |0010\rangle + |0011\rangle + |1101\rangle + \\
&+ |1100\rangle - |0100\rangle + |0101\rangle + |1011\rangle + |1010\rangle + |0110\rangle - |0111\rangle + |1001\rangle + |1000\rangle\Big) \\
&= \frac{1}{4\sqrt{2}}\Big((1-i)|0000\rangle + (-1-i)|0001\rangle + (1+i)|1111\rangle + (1-i)|1110\rangle + \\
&+ (-1-i)|0010\rangle + (1-i)|0011\rangle + (+1-i)|1101\rangle + (1+i)|1100\rangle + \\
&+ (-1-i)|0100\rangle + (1-i)|0101\rangle + (1-i)|1011\rangle + (1+i)|1010\rangle + (1-i)|0110\rangle + \\
&+ (-1-i)|0111\rangle + (1+i)|1001\rangle + (1-i)|1000\rangle\Big),
\end{aligned}
$$

da cui, esprimendo le ampiezze complesse in forma esponenziale e associando ad ogni stato di base il corrispondente numero decimale, si ottiene che

$$
\begin{aligned}
|\tilde{\psi}^y_+\rangle = \frac{1}{4}\Big(&e^{i\frac{7\pi}{4}}|0\rangle + e^{i\frac{5\pi}{4}}|1\rangle + e^{i\frac{5\pi}{4}}|2\rangle + e^{i\frac{7\pi}{4}}|3\rangle + e^{i\frac{5\pi}{4}}|4\rangle + e^{i\frac{7\pi}{4}}|5\rangle + e^{i\frac{7\pi}{4}}|6\rangle + e^{i\frac{5\pi}{4}}|7\rangle + \\
&+ e^{i\frac{7\pi}{4}}|8\rangle + e^{i\frac{\pi}{4}}|9\rangle + e^{i\frac{\pi}{4}}|10\rangle + e^{i\frac{7\pi}{4}}|11\rangle + e^{i\frac{\pi}{4}}|12\rangle + e^{i\frac{7\pi}{4}}|13\rangle + e^{i\frac{7\pi}{4}}|14\rangle + e^{i\frac{\pi}{4}}|15\rangle\Big).
\end{aligned}
$$

Analogamente, si ha che

$$
\begin{aligned}
|\tilde{\psi}^y_-\rangle = \frac{1}{4}\Big(&e^{i\frac{\pi}{4}}|0\rangle + e^{i\frac{3\pi}{4}}|1\rangle + e^{i\frac{3\pi}{4}}|2\rangle + e^{i\frac{\pi}{4}}|3\rangle + e^{i\frac{3\pi}{4}}|4\rangle + e^{i\frac{\pi}{4}}|5\rangle + e^{i\frac{\pi}{4}}|6\rangle + e^{i\frac{3\pi}{4}}|7\rangle + \\
&+ e^{i\frac{5\pi}{4}}|8\rangle + e^{i\frac{3\pi}{4}}|9\rangle + e^{i\frac{3\pi}{4}}|10\rangle + e^{i\frac{5\pi}{4}}|11\rangle + e^{i\frac{3\pi}{4}}|12\rangle + e^{i\frac{5\pi}{4}}|13\rangle + e^{i\frac{5\pi}{4}}|14\rangle + e^{i\frac{3\pi}{4}}|15\rangle\Big).
\end{aligned}
$$

A questo punto, si procede sostituendo nella (4.16) le espressioni ottenute per $|\tilde{\psi}^{x,y}_\pm\rangle$. Notando che, posto $\Xi^z = \sigma^z_1\sigma^z_2\sigma^z_3\sigma^z_4$,

$$
\begin{aligned}
&\Xi^z|0\rangle = \Xi^z|0000\rangle = +|0\rangle, \quad \Xi^z|1\rangle = \Xi^z|0001\rangle = -|1\rangle, \quad \Xi^z|2\rangle = \Xi^z|0010\rangle = -|2\rangle, \\
&\Xi^z|3\rangle = \Xi^z|0011\rangle = +|3\rangle, \quad \Xi^z|4\rangle = \Xi^z|0100\rangle = -|4\rangle, \quad \Xi^z|5\rangle = \Xi^z|0101\rangle = +|5\rangle, \\
&\Xi^z|6\rangle = \Xi^z|0110\rangle = +|6\rangle, \quad \Xi^z|7\rangle = \Xi^z|0111\rangle = -|7\rangle, \quad \Xi^z|8\rangle = \Xi^z|1000\rangle = -|8\rangle, \\
&\Xi^z|9\rangle = \Xi^z|1001\rangle = +|9\rangle, \quad \Xi^z|10\rangle = \Xi^z|1010\rangle = +|10\rangle, \\
&\Xi^z|11\rangle = \Xi^z|1011\rangle = -|11\rangle, \quad \Xi^z|12\rangle = \Xi^z|1100\rangle = +|12\rangle, \\
&\Xi^z|13\rangle = \Xi^z|1101\rangle = -|13\rangle, \quad \Xi^z|14\rangle = \Xi^z|1110\rangle = -|14\rangle, \\
&\Xi^z|15\rangle = \Xi^z|1111\rangle = +|15\rangle,
\end{aligned}
\tag{A.1}
$$

considerando l'ortonormalità della base computazionale si ottiene che

$$
\langle\tilde{\psi}^x_+|\Xi^z|\tilde{\psi}^x_+\rangle = \Big(\frac{1}{2\sqrt{2}}\Big)^2(1+1+1+1+1+1+1+1) = +1,
$$

$$
\langle\tilde{\psi}^x_-|\Xi^z|\tilde{\psi}^x_-\rangle = \Big(\frac{-1}{2\sqrt{2}}\Big)^2(-1-1-1-1-1-1-1-1) = -1,
$$

$$
\langle\tilde{\psi}^y_+|\Xi^z|\tilde{\psi}^y_+\rangle = \Big(\frac{1}{4}\Big)^2(+1-1-1+1-1+1+1-1-1+1+1-1+1-1-1+1) = 0,
$$

$$
\langle\tilde{\psi}^y_-|\Xi^z|\tilde{\psi}^y_-\rangle = \Big(\frac{1}{4}\Big)^2(+1-1-1+1-1+1+1-1-1+1+1-1+1-1-1+1) = 0.
$$

Appendice B

Dati sperimentali e propagazione degli errori

Riporto in forma di tabella i valori ottenuti con `ibmq_santiago` per $\langle\Sigma^x_+\rangle = \langle\psi_+|\Sigma^x|\psi_+\rangle$, $\langle\Sigma^x_-\rangle = \langle\psi_-|\Sigma^x|\psi_-\rangle$, $\langle\Sigma^y_+\rangle = \langle\psi_+|\Sigma^y|\psi_+\rangle$, $\langle\Sigma^y_-\rangle = \langle\psi_-|\Sigma^y|\psi_-\rangle$. L'errore associato a ciascun valore è stato calcolato come:

$$\Delta\Sigma^{x,y}_{\pm} = \langle\Sigma^{x,y}_{\pm}\rangle\,\Delta,$$

con Δ errore relativo totale (vedi equazione (5.8)).

ω	$\langle\Sigma^x_+\rangle$	$\langle\Sigma^x_-\rangle$	$\langle\Sigma^y_+\rangle$	$\langle\Sigma^y_-\rangle$
1	0.78 ± 0.09	0	-0.0066 ± 0.0007	0
0.9375	0.79 ± 0.09	-0.82 ± 0.09	-0.016 ± 0.002	0.0039 ± 0.0004
0.875	0.77 ± 0.09	-0.81 ± 0.09	-0.019 ± 0.002	-0.0078 ± 0.0009
0.8125	0.79 ± 0.09	-0.70 ± 0.08	-0.037 ± 0.004	-0.060 ± 0.007
0.75	0.81 ± 0.09	-0.75 ± 0.08	-0.025 ± 0.003	0.050 ± 0.006
0.6875	0.75 ± 0.08	-0.81 ± 0.09	-0.032 ± 0.004	0.080 ± 0.009
0.625	0.81 ± 0.09	-0.82 ± 0.09	-0.036 ± 0.004	-0.011 ± 0.001
0.5625	0.81 ± 0.09	-0.81 ± 0.09	0.018 ± 0.002	0.037 ± 0.004
0.5	0.80 ± 0.09	-0.79 ± 0.09	-0.040 ± 0.004	0.0068 ± 0.0008
0.4375	0.79 ± 0.09	-0.80 ± 0.09	-0.09 ± 0.01	0.062 ± 0.007
0.375	0.79 ± 0.09	-0.78 ± 0.09	-0.061 ± 0.007	0.021 ± 0.002
0.3125	0.76 ± 0.08	-0.79 ± 0.09	0.0031 ± 0.0003	0.013 ± 0.001
0.25	0.80 ± 0.09	-0.79 ± 0.09	-0.024 ± 0.003	0.0065 ± 0.0007
0.1875	0.78 ± 0.09	-0.81 ± 0.09	0.0026 ± 0.0003	0.047 ± 0.005
0.125	0.79 ± 0.09	-0.79 ± 0.09	-0.066 ± 0.007	0.0028 ± 0.0003
0.0625	0.81 ± 0.09	-0.79 ± 0.09	0.10 ± 0.01	0.029 ± 0.003
0	0	-0.80 ± 0.09	0	0.044 ± 0.005

Tabella B.1

I valori medi $\langle\Sigma^x\rangle$, $\langle\Sigma^y\rangle$ sono stati calcolati a partire dai dati riportati in tabella B.1 applicando le equazioni (5.2). I valori ottenuti sono riportati nella tabella B.2. Gli errori associati sono frutto di una somma in quadratura:

$$\Delta\Sigma^{x,y} = \sqrt{\omega^2(\Delta\Sigma^{x,y}_+)^2 + (1-\omega)^2(\Delta\Sigma^{x,y}_-)^2}.$$

ω	$\langle\Sigma^x\rangle$	$\langle\Sigma^y\rangle$
1	0.78 ± 0.09	-0.0066 ± 0.0007
0.9735	0.69 ± 0.08	-0.015 ± 0.002
0.875	0.58 ± 0.08	-0.017 ± 0.002
0.8125	0.51 ± 0.07	-0.042 ± 0.004
0.75	0.42 ± 0.07	-0.007 ± 0.003
0.6875	0.26 ± 0.06	0.003 ± 0.004
0.625	0.20 ± 0.07	-0.027 ± 0.003
0.5625	0.10 ± 0.06	0.027 ± 0.002
0.5	0.00 ± 0.06	-0.017 ± 0.002
0.4375	-0.11 ± 0.06	-0.004 ± 0.006
0.375	-0.19 ± 0.06	-0.010 ± 0.003
0.3125	-0.30 ± 0.07	0.010 ± 0.001
0.25	-0.39 ± 0.07	-0.0012 ± 0.0009
0.1875	-0.51 ± 0.07	0.039 ± 0.004
0.125	-0.59 ± 0.08	-0.006 ± 0.001
0.0625	-0.69 ± 0.08	0.034 ± 0.003
0	-0.80 ± 0.09	0.044 ± 0.005

Tabella B.2

Infine, i valori di $E(\rho_{exp})$ riportati nella tabella 5.4 sono stati calcolati sostituendo i valori della tabella B.2 nella (4.3). Gli errori associati sono stati calcolati come

$$\Delta E = \sqrt{\left|\frac{\partial E}{\partial \langle\Sigma^x\rangle}\right|^2 (\Delta\Sigma^x)^2 + \left|\frac{\partial E}{\partial \langle\Sigma^y\rangle}\right|^2 (\Delta\Sigma^y)^2} = \sqrt{\frac{(\Delta\Sigma^x)^2 \langle\Sigma^x\rangle^2 + (\Delta\Sigma^y)^2 \langle\Sigma^y\rangle^2}{4(1 - \langle\Sigma^x\rangle^2 - \langle\Sigma^y\rangle^2)}}.$$

Bibliografia

[1] V.M. Tkachuk A.R. Kuzmak. «Measuring entanglement of a rank-2 mixed state prepared on a quantum computer». In: *Eur. Phys. J. Plus* 136.564 (2021). DOI: https://doi.org/10.1140/epjp/s13360-021-01553-2.

[2] MD SAJID ANIS et al. *Qiskit: An Open-source Framework for Quantum Computing*. 2021. DOI: 10.5281/zenodo.2573505.

[3] Abraham Asfaw et al. *Learn Quantum Computation Using Qiskit*. 2020. URL: http://community.qiskit.org/textbook.

[4] Charles H. Bennett et al. «Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels». In: *Phys. Rev. Lett.* 70 (13 1993), pp. 1895–1899. DOI: 10.1103/PhysRevLett.70.1895. URL: https://link.aps.org/doi/10.1103/PhysRevLett.70.1895.

[5] B. Diu e F. Laloe C.Cohen-Tannoudji. *Quantum Mechanics*. Vol. 1. John Wiley & Sons, 2003. ISBN: 0-471-16432-1.

[6] Andrew W. Cross et al. *Open Quantum Assembly Language*. 2017. arXiv: 1707.03429 [quant-ph].

[7] David P. DiVincenzo. «The Physical Implementation of Quantum Computation». In: *Fortschritte der Physik* 48.9-11 (2000), pp. 771–783. ISSN: 1521-3978. DOI: 10.1002/1521-3978(200009)48:9/11<771::aid-prop771>3.0.co;2-e. URL: http://dx.doi.org/10.1002/1521-3978(200009)48:9/11%3C771::AID-PROP771%3E3.0.CO;2-E.

[8] N. Gisin e A. Tavakoli E. Bäumer. «Demonstrating the power of quantum computers, certification of highly entangled measurements and scalable quantum nonlocality». In: *npj Quantum Inf* 7 (2021), p. 117. DOI: https://doi.org/10.1038/s41534-021-00450-x.

[9] A. Einstein, B. Podolsky e N. Rosen. «Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?» In: *Phys. Rev.* 47 (10 1935), pp. 777–780. DOI: 10.1103/PhysRev.47.777. URL: https://link.aps.org/doi/10.1103/PhysRev.47.777.

[10] R.P. Feynman. «Simulating physics with computers». In: *Int J Theor Phys* 21 (1982), pp. 467–488. DOI: https://doi.org/10.1007/BF02650179.

[11] Andrzej Frydryszak, Mykola Samar e V. Tkachuk. «Quantifying geometric measure of entanglement by mean value of spin and spin correlations with application to physical systems». In: *The European Physical Journal D* 71 (set. 2017), p. 233. DOI: 10.1140/epjd/e2017-70752-3.

[12] Ryszard Horodecki et al. «Quantum entanglement». In: *Rev. Mod. Phys.* 81 (2 2009), pp. 865–942. DOI: 10.1103/RevModPhys.81.865. URL: https://link.aps.org/doi/10.1103/RevModPhys.81.865.

[13] Farzan Jazaeri et al. *A Review on Quantum Computing: Qubits, Cryogenic Electronics and Cryogenic MOSFET Physics*. 2019. arXiv: 1908.02656 [quant-ph].

[14] Richard Jozsa e Noah Linden. «On the role of entanglement in quantum-computational speed-up». In: *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences* 459.2036 (2003), pp. 2011–2032. ISSN: 1471-2946. DOI: 10.1098/rspa.2002.1097. URL: http://dx.doi.org/10.1098/rspa.2002.1097.

[15] P. Krantz et al. «A quantum engineer's guide to superconducting qubits». In: *Applied Physics Reviews* 6.2 (2019), p. 021318. DOI: 10.1063/1.5089550. URL: https://doi.org/10.1063/1.5089550.

[16] B. P. Lanyon et al. «Experimental Violation of Multipartite Bell Inequalities with Trapped Ions». In: *Phys. Rev. Lett.* 112 (10 2014), p. 100403. DOI: 10.1103/PhysRevLett.112.100403. URL: https://link.aps.org/doi/10.1103/PhysRevLett.112.100403.

[17] I.L. Nielsen M.A. e Chuang. *Quantum Computation and Quantum Information*. 10th Anniversary Edition. Cambridge University Press, 2010. ISBN: 978-1-107-00217-3.

[18] Gabriel Popkin. «Quest for qubits». In: *Science* 354.6316 (2016), pp. 1090–1093. ISSN: 0036-8075. DOI: 10.1126/science.354.6316.1090. eprint: https://science.sciencemag.org/content/354/6316/1090.full.pdf. URL: https://science.sciencemag.org/content/354/6316/1090.

[19] John Preskill. *Lecture Notes for Ph219/CS219: Quantum Information and Computation*. California Institute of Technology, 2001. Cap. 4 (Quantum Entanglement). URL: http://theory.caltech.edu/~preskill/ph229/. (ultima data di consultazione: 28.06.2021).

[20] John Preskill. *Lecture Notes for Ph219/CS219: Quantum Information and Computation*. California Institute of Technology, 2015. Cap. 5 (Quantum Information Theory). URL: http://theory.caltech.edu/~preskill/ph229/. (ultima data di consultazione: 28.06.2021).

[21] IBM Quantum. URL: https://quantum-computing.ibm.com/. (ultima data di consultazione: 15.09.2021).

[22] W. Rieffel E. e Polak. *Quantum Computing. A Gentle Introduction*. Massachusetts Institute of Technology, 2011. ISBN: 978-0-262-01506-6.

[23] E. Schrödinger. «Die gegenwärtige Situation in der Quantenmechanik». In: *Naturwissenschaften* 23 (1935), pp. 844–849. DOI: https://doi.org/10.1007/BF01491987.

[24] E. Schrödinger. «Discussion of Probability Relations between Separated Systems». In: *Mathematical Proceedings of the Cambridge Philosophical Society* 31.4 (1935), pp. 555–563. DOI: 10.1017/S0305004100013554.

[25] Qiskit Development Team. URL: https://qiskit.org/documentation/. (ultima data di consultazione: 10.09.2021).

[26] Tzu-Chieh Wei e Paul M. Goldbart. «Geometric measure of entanglement and applications to bipartite and multipartite quantum states». In: *Physical Review A* 68.4 (2003). ISSN: 1094-1622. DOI: 10.1103/physreva.68.042307. URL: http://dx.doi.org/10.1103/PhysRevA.68.042307.

[27] Robert Wille, Rod Van Meter e Yehuda Naveh. «IBM's Qiskit Tool Chain: Working with and Developing for Real Quantum Computers». In: *2019 Design, Automation Test in Europe Conference Exhibition (DATE)*. 2019, pp. 1234–1240. DOI: 10.23919/DATE.2019.8715261.

[28] William K. Wootters e W. S. Leng. «Quantum Entanglement as a Quantifiable Resource [and Discussion]». In: *Philosophical Transactions: Mathematical, Physical and Engineering Sciences* 356.1743 (1998), pp. 1717–1731. ISSN: 1364503X. URL: http://www.jstor.org/stable/55007.