# Quantum Computing

Alessandra Di Pierro

## Introduzione alla meccanica quantistica

Fino ad ora abbiamo parlato di sistemi quantistici, stati quantistici, evoluzione e misurazione di stati quantistici, ecc., ma non abbiamo ancora definito questi termini in modo formale. Un modello matematico che ci permette di farlo é la teoria quantistica.

## 1 I postulati della meccanica quantistica

La meccanica quantistica fornisce la descrizione piú accurata e completa delle leggi che governano il mondo fisico. Il formalismo matematico su cui si basa e la realtá fisica che descrive sono messi in relazione mediante alcuni postulati fondamentali.

**Postulato 1** Ogni sistema fisico isolato ha associato uno spazio di Hilbert complesso, detto *spazio degli stati* del sistema. Il sistema é completamente descritto dal suo *vettore di stato*, che é un vettore unitario nello spazio degli stati.

Il sistema fisico isolato piú semplice é il *qubit*. Lo spazio di Hilbert associato é $\mathbb{C}^2$. La base computazionale formata da $|0\rangle$ e $|1\rangle$ é una base ortonormale e la condizione che ogni vettore $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ (con $a, b \in \mathbb{C}$) sia un vettore unitario é espressa equivalentemente da $|a|^2 + |b|^2 = 1$, oppure mediante il prodotto interno da $\langle\psi\rangle = 1$. Ricordiamo che $a$ e $b$ sono chiamate le *ampiezze* rispettivamente del vettore $|0\rangle$ e del vettore $|1\rangle$. Osserviamo inoltre che uno stato di un sistema quantistico é in realtá una classe di equivalenza di vettori che differiscono per moltiplicazione di uno scalare complesso non nullo; il vettore unitario é il rappresentante di questa classe. Quindi lo stato $e^{i\theta}\,|\psi\rangle$, dove $|\psi\rangle$ é uno stato e $\theta$ é un numero reale, é equivalente a $|\psi\rangle$. Il fattore $e^{i\theta}$ é detto *fattore di fase globale*. Questa identificazione degli stati con fasi globali diverse é giustificata dal fatto che le statistiche di *misurazione* (cf.

Postulato 3) di questi stati sono le stesse. Un altro tipo di fattore, detto *fase relativa*, é invece fisicamente significativo e due stati che differiscono per un fattore di fase relativa non possono essere identificati. Ad esempio, identifichiamo $a\,|\varphi\rangle + b\,|\psi\rangle$ con $e^{i\theta}(a\,|\varphi\rangle + b\,|\psi\rangle)$ ma non con $a\,|\varphi\rangle + e^{i\theta} b\,|\psi\rangle$.

**Postulato 2** L'evoluzione di un sistema quantistico *chiuso* é descritto da una *trasformazione unitaria*: lo stato $|\psi\rangle$ del sistema al tempo $t_1$ é in relazione con lo stato $|\psi'\rangle$ del sistema al tempo $t_2$ mediante un operatore unitario $U$ che dipende solo da $t_1$ e $t_2$,

$$\left|\psi'\right\rangle = U\,|\psi\rangle\,.$$

Per il semplice sistema quantistico rappresentato da un qubit abbiamo visto vari esempi di operatori unitari: le matrici di Pauli,

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

e la porta di Hadamard

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

$X$ é detta anche porta logica `NOT` e $Y$ corrisponde a $iZX$.
Una versione piú raffinata di questo postulato descrive l'evoluzione di un sistema quantistico chiuso in *tempo continuo*. Diamo questa versione nel Postulato 2' per completezza, ma non ne faremo uso negli argomenti che tratteremo successivamente, in cui faremo sempre uso della formulazione unitaria della dinamica quantistica.

**Postulato 2'** L'evoluzione nel tempo dello stato di un sistema quantistico chiuso é descritta dall'*equazione di Schrödinger*

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

dove $\hbar$é una costante fisica, nota come la *costante di Planck*, il cui valore deve essere determinato sperimentalmente. $H$é un operatore Hermitiano fissato, noto come l'*Hamiltoniano* del sistema chiuso.

In generale, trovare l' Hamiltoniano di un sistema, cioé l'operatore che ne descrive completamente la dinamica, é un problema molto difficile che richiede un numero sostanziale di esperimenti per poter essere risolto. Noi non ci

porremo questo tipo di problemi; per i nostri scopi ci basterá sapere che ogni operatore unitario $U$ (del tipo di quelli che useremo per descrivere una computazione quantistica) puó essere realizzato come una soluzione dell'equazione di Shröndinger e che esiste una corrispondenza biunivoca tra la descrizione della dinamica di un sistema a *tempo discreto* mediante operatori unitari e la descrizione a *tempo continuo* mediante gli Hamiltoniani.

**Postulato 3** Ogni *osservabile* $M$ (cioé ogni proprietá di un sistema fisico che puó essere misurata) é rappresentato da un operatore Hermitiano sullo spazio degli stati del sistema che viene osservato e viceversa. $M$ ha la forma

$$M = \sum_m m P_m,$$

dove $P_m$ é la proiezione sul sottospazio degli autovettori di $M$ corrispondenti all'autovalore $m$ (ricordiamo che gli autovalori di operatori Hermitiani sono reali, cf. Appendice). I possibili risultati di una misura dell'osservabile $M$ corrispondono agli autovalori $m$ di $M$. Dopo una misura di $M$ nello stato $\psi$, la probabilitá di ottenere il risultato $m$ é

$$p(m) = \langle\psi| P_m |\psi\rangle = \| P_m |\psi\rangle \|^2.$$

Lo stato del sistema immediatamente dopo una misura con risultato $m$ é

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

Gli operatori $P_m$ soddisfano l'equazione di completezza

$$\sum_m P_m = I.$$

L'equazione di completezza esprime il fatto che la somma delle probabilitá dei risultati di una misura deve essere 1. Infatti:

$$1 = \sum_m p(m) = \sum_m \langle\psi| P_m |\psi\rangle = \langle\psi|\psi\rangle.$$

Questo tipo di misurazione viene spesso chiamata *misurazione proiettiva* perché l'osservabile $M$ é determinato da un qualsiasi insieme di operatori di proiezione ortogonali $P_m$ che soddisfano la relazione di completezza e tali che $P_m P_{m'} = \delta_{mm'} P_m$. Misurare nella base $\{|m\rangle\}$, dove $\{|m\rangle\}$ é una base ortonormale, significa eseguire una misurazione proiettiva con operatori di proiezione $|m\rangle\langle m|$.

**Esempio 1.1 (qubit)** *Consideriamo l'osservabile* $M \equiv 0P_0 + 1P_1$ *e misuriamolo nello stato* $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. *Otterremo il risultato* 0 *con probabilitá*

$$p(0) = \|P_0|\psi\rangle\|^2 = \||0\rangle\langle 0|\psi\rangle\|^2 = |a|^2$$

*e analogamente*

$$p(1) = \|P_1|\psi\rangle\|^2 = \||1\rangle\langle 1|\psi\rangle\|^2 = |b|^2.$$

*Inoltre, se abbiamo osservato* 0 *allora lo stato* $|\psi\rangle$ *diventerá* $|0\rangle = |0\rangle\langle 0|\psi\rangle$, *mentre se il risultato era* 1 *diventerá* $|1\rangle = |1\rangle\langle 1|\psi\rangle$.

Il risultato della misura di un osservabile $M$ in uno stato $|\psi\rangle$ é in generale aleatorio. Una formula utile per determinare il valore medio del risulato della misura di $M$ si ottiene mediante la nozione nota in teoria della probabilitá come *media* o *speranza*, $\mathbf{E}$, di una variabile aleatoria (nel nostro caso l'osservabile $M$), corrispondente alla media su tutti i possibili risultati, pesata dalle probabilitá associate:

$$\begin{aligned}
\mathbf{E}_{|\psi\rangle}(M) &= \sum_m mp(m) \\
&= \sum_m m\langle\psi|P_m|\psi\rangle \\
&= \langle\psi|\left(\sum_m P_m\right)|\psi\rangle \\
&= \langle\psi|M|\psi\rangle .
\end{aligned}$$

Il valore medio di un osservabile $M$ si indica spesso con la notazione $< M >$.

**Esempio 1.2** *Si vuole misurare l'osservabile* $Z$ *nello stato* $|\psi\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$. *Poiché* $Z$ *ha autovalori* $+1$ *e* $-1$ *con corrispondenti autovettori* $|0\rangle$ *e* $|1\rangle$, *si ha che*

$$Z = |0\rangle\langle 0| - |1\rangle\langle 1| .$$

*I possibili risultati sono quindi* 1 *e* $-1$ *con probabilitá* $p(1) = \langle\psi|0\rangle\langle 0|\psi\rangle = \frac{1}{2}$ *e* $p(-1) = \langle\psi|1\rangle\langle 1|\psi\rangle = \frac{1}{2}$, *con valore medio* $< Z >= 0$. *Lo stato dopo la misurazione risulterá*

$$\begin{aligned}
&\textit{se } m = 1 \qquad \sqrt{2}(|0\rangle\langle 0|\psi\rangle) = |0\rangle \\
&\textit{se } m = -1 \qquad \sqrt{2}(|1\rangle\langle 1|\psi\rangle) = |1\rangle .
\end{aligned}$$

**Postulato 4** Lo spazio degli stati di un sistema fisico composto é il prodotto tensore degli spazi degli stati dei sistemi fisici componenti. Se il sistema é composto da $n$ sottosistemi e il componente $i$-esimo si trova nello stato $|\psi_i\rangle$, allora lo stato del sistema totale é $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$.

Questo postulato descrive come costruire lo spazio degli stati di un sistema quantistico composto da due o piú sistemi fisici distinti a partire dagli spazi degli stati dei sistemi componenti.

**Esercizio 1.3** *Dato un sistema di due qubits, dimostrare che il valore medio dell'osservabile $X_1 Z_2$ misurato nello stato $(|00\rangle + |11\rangle)/\sqrt{2}$ é zero. La notazione $X_1$ e $Z_2$ indica rispettivamente l'operatore di Pauli $X$ applicato al primo qubit e l'operatore di Pauli $Z$ applicato al secondo qubit.*

Il Postulato 4 permette di definire la nozione di *entanglement* che, insieme al problema della misurazione, rappresenta una delle proprietá piú discusse dei sistemi quantistici. Uno stato di un sistema composto si dice "entangled" se non puó essere scritto come prodotto dei suoi sistemi componenti.

**Esercizio 1.4** *Considera il seguente stato di un registro di due qubit:*

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

*Dimostrare che non esistono stati $|a\rangle$ e $|b\rangle$ dei due qubit componenti tali che $|\psi\rangle = |a\rangle\,|b\rangle$.*

Come giá visto nell'esempio del teletrasporto, gli stati entangled possono essere utilizzati per ottenere dei risultati sorprendenti (come la trasmissione dello stato di un qubit attraverso due soli bit di informazione classica). Nella sezione 2 viene presentato un altro esempio in cui l'entanglement viene utilizzato per comunicare due bit di informazione classica attraverso la trasmissione di un solo qubit. L'esempio illustra anche l'applicazione del Postulato 3.

## 1.1 Il problema della misurazione quantistica

Il problema della misurazione quantistica diede luogo ad accesi dibattiti sin dalla nascita della teoria quantistica nel 1920. John von Neumann introdusse il primo trattamento assiomatico rigoroso della meccanica quantistica nel 1955, intervenendo in maniera decisiva anche sul problema della misurazione

e fornendo una spiegazione chiara ai vari paradossi che erano stati introdotti per sostenere l'inadeguatezza della teoria quantistica.

Secondo la formalizzazione di von Neumann il processo di misurazione avviene in due fasi. Nella prima fase l'operatore Hermitiano che rappresenta l'osservabile viene applicato allo stato del sistema generando uno stato entangled. In una seconda fase avviene il cosiddetto "quantum leap" o "riduzione di stato", cioé il salto dallo stato enatngled allo stato corrispondente ad uno degli autovettori dell'osservabile. Questa riduzione é nondeterministica e conseguentemente non c'e' modo di prevedere quale dei risultati sará ottenuto prima che il processo di misurazione abbia termine. In altre parole, per un osservabile non é mai possibile stabilire in maniera definita il valore che verrá misurato. La meccanica quantistica fornisce tuttavia delle informazioni statistiche sui possibili risultati di una misurazione secondo quella che é nota come l'*interpretazione statistica di Born*. Attraverso misurazioni fatte su copie del sistema opportunamente preparate, é possibile stabilire la distribuzione probabilistica dei risultati. Il significato di *probabilitá* di un risultato va inteso secondo l'interpretazione data in teoria delle probabilitá come *frequenza relativa*: la probabilitá di un risultato e' il rapporto tra il numero delle volte che l'esperimento ha successo (cioé si ottiene quel risultato) e il numero totale degli esperimenti fatti, purché si ripeta l'esperimento un numero sufficientemente grande di volte.

## 2 Un'applicazione: Codifica superdensa

Alice deve comunicare a Bob l'informazione contenuta in due bit classici, (cioé un numero tra $0, 1, 2, 3$) e deve farlo trasmettendo un solo qubit. Poiché la misurazione di un qubit puó dare come risultato solo un bit di informazione classica (0 o 1), questo compito sembrerebbe impossibile. In realtá il problema puó essere risolto attraverso l'uso di una coppia EPR. Supponiamo che inizialmente Alice e Bob sono in possesso rispettivamente del primo e del secondo qubit della coppia entangled

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Alice applica al suo qubit una delle trasformazioni $I, X, iY, Z$ a seconda del numero che vuole trasmettere. In particolare, lo stato $|\psi\rangle$ viene trasformato nel seguente modo:

$$0 \quad : \quad |\psi\rangle \to (I \otimes I)\,|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$
\begin{aligned}
1 \quad &: \quad |\psi\rangle \to (X \otimes I)\,|\psi\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\
2 \quad &: \quad |\psi\rangle \to (iY \otimes I)\,|\psi\rangle = \frac{-|10\rangle + |01\rangle}{\sqrt{2}} \\
3 \quad &: \quad |\psi\rangle \to (Z \otimes I)\,|\psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}
\end{aligned}
$$

I quattro stati risultanti formano una base ortonormale nota come *base di Bell*. Allora Alice non deve fare altro che inviare il suo qubit a Bob, il quale puó ora determinare i due bits che Alice voleva trasmettergli, semplicemente attraverso una misura nella base di Bell. Piú precisamente, indicando con $|\beta_0\rangle, |\beta_1\rangle, |\beta_2\rangle, |\beta_3\rangle$ i quattro stati di Bell, per ricevere l'informazione Bob deve misurare un osservabile del tipo

$$M \equiv \sum_{i=0}^{3} i\,|\beta_i\rangle\,\langle\beta_i|$$

nello stato dei due qubit in suo possesso. Nota che il risultato della misura ha sempre probabilitá 1. Infatti, la probabilitá di ottenere $i$ nello stato $|\beta_j\rangle$ é data da

$$p(i) = \langle\beta_j|\,\beta_i\rangle\,\langle\beta_i|\,\beta_j\rangle = \begin{cases} 1 & \text{se } i = j \\ 0 & \text{se } i \neq j \end{cases}$$

**Esercizio 2.1** *Verificare che Bob puó determinare i due bits attraverso misurazioni su un singolo qubit. (Suggerimento: misurare il secondo qubit e applicare Hadamard al primo qubit dello stato risultante).*

# A Richiami di Algebra Lineare

## A.1 Prodotto interno e spazi di Hilbert

Dato uno spazio vettoriale $V$, una funzione $(\cdot,\cdot) : V \times V \mapsto \mathbb{C}$ é un *prodotto interno* (o *prodotto scalare*) se soddisfa i seguenti requisiti:

- $(|v\rangle, |v\rangle) \geq 0$
- $(|v\rangle, |v\rangle) = 0$ se e solo se $v = 0$
- $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$
- $(|v\rangle, \sum_i a_i\,|w_i\rangle) = \sum_i a_i(|v\rangle, |w_i\rangle)$.

**Esercizio A.1** *Verificare che la funzione definita da*

$$((y_1, y_2, \ldots, y_n), (z_1, z_2, \ldots, z_n)) = \sum_{i=1}^{n} y_i^* z_i,$$

*dove* $(y_1, y_2, \ldots, y_n)$ *e* $(z_1, z_2, \ldots, z_n)$ *sono vettori in* $\mathbb{C}^n$*,é un prodotto interno.*

Dalla definizione segue che ogni prodotto interno soddisfa la seguente proprietà:

$$(\sum_i a_i \left|w_i\right\rangle, \left|v\right\rangle) = \sum_i a_i^* (\left|w_i\right\rangle, \left|v\right\rangle).$$

In notazione di Dirac, il prodotto interno del vettore $\left|v\right\rangle$ con il vettore $\left|w\right\rangle$é denotato da $\left\langle v\right| \left. w\right\rangle$. Mediante il prodotto interno si può definire la *norma* di un vettore come

$$\|v\| = \sqrt{\left\langle v\right\rangle}.$$

Uno *spazio di Hilbert*, é uno spazio vettoriale $V$ dotato di prodotto interno e completo rispetto alla metrica indotta dalla norma $\|\cdot\|$. Per completezza si intende che tutte le sequenze di Cauchy di vettori in $V$ convergono a un limite in $V$. Questa proprietà é significativa nel caso di spazi a dimensioni infinite, poichè per spazi vettoriali di dimensioni finite é sempre soddisfatta. In computazione quantistica, gli spazi vettoriali con cui si ha a che fare sono sempre di dimensioni finite. Pertanto, per i nostri scopi, il termine "spazio di Hilbert" sarà del tutto equivalente a "spazio vettoriale con prodotto interno". Inoltre, ci riferiremo di solito ad uno spazio vettoriale $V$, intendendo implicitamente che $V$é uno spazio di Hilbert.

## A.2 Basi ortonormali

Un vettore $\left|v\right\rangle$ in uno spazio vettoriale $V$ si dice *vettore unitario* o *normalizzato* se la sua normaé 1, cioè $\|v\| = 1$. I vettori $\left|v\right\rangle$ e $\left|w\right\rangle$ si dicono *ortogonali* se il loro prodotto internoé zero, cioè $\left\langle v\right| \left. w\right\rangle = 0$. Un insieme di vettori $\{\left|i\right\rangle\}$ con indice $i$ si dice *ortonormale* se per ogni $i$, $\{\left|i\right\rangle\}$ é un vettore unitario e vettori distinti sono a due a due ortogonali, cioè

$$\left\langle i\right| \left. j\right\rangle = \delta_{ij} = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

È sempre possile trasformare una qualsiasi base per uno spazio vettoriale $V$ in una base ortonormale. Il metodo per farlo si chiama *procedura di*

*Gram-Schmidt* e non lo esamineremo in dettaglio. Grazie a questa procedura possiamo assumere che le basi che considereremo d'ora in poi siano sempre ortonormali.

## A.3 Operatori lineari e prodotto esterno

Una rappresentazione utile di un operatore lineare é quella mediante *prodotto esterno*. Dati $|v\rangle \in V$ e $|w\rangle \in W$, definiamo l'operatore lineare $|w\rangle\langle v| : V \mapsto W$ associa ad ogni vettore $|v'\rangle \in V$ il vettore in $W$ risultante dalla moltiplicazione scalare di $w$ per il prodotto interno $\langle v|\, v'\rangle$, cioè

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

Ogni base ortonormale $\{|i\rangle\}$ per uno spazio vettoriale $V$ soddisfa la *relazione di completezza*

$$\sum_i |i\rangle\langle i| = I.$$

Infatti, per ogni $|v\rangle \in V$, $|v\rangle = \sum_i v_i\,|i\rangle$, si ha che

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|\, v\rangle = \sum_i v_i\,|i\rangle = |v\rangle\,,$$

poichè $\langle i|\, v\rangle = v_i$ per ogni $i$.
Utilizzando la relazione di completezza si ottiene la seguente rappresentazione per operatori lineari che sarà molto utile nel seguito.
Dato un operatore lineare $L : V \mapsto W$ e date le basi ortonormali $\{|v_i\rangle\}$ per $V$ e $\{|w_j\rangle\}$ per $W$, possiamo scrivere $L$ come

$$L = I_W L I_V,$$

dove $I_V$ e $I_W$ sono rispettivamente l'identità in $V$ e in $W$. Da questa espressione si ottiene la rappresentazione in forma di prodotto esterno di $L$. Infatti,

$$I_W L I_V = \sum_{ij} |w_j\rangle\langle w_j|\, L\,|v_i\rangle\langle v_i| = \sum_{ij} \langle w_j|\, L\,|v_i\rangle\, |w_j\rangle\langle v_i|\,.$$

Nota che i coefficienti $\langle w_j|\, L\,|v_i\rangle$ corrispondono agli elementi della matrice di rappresentazione di $L$ rispetto alla base di input $\{|v_i\rangle\}$ e alla base di output $\{|w_j\rangle\}$. In particolare, $L\,|v_i\rangle$ é la trasformazione dell'$i$-esimo vettore della base di input in un vettore in $W$ la cui coordinata $j$-esimaé data da $\langle w_j|\, L\,|v_i\rangle$. Tale elementoé pertanto l'elemento della colonna $i$ e della riga $j$ della matrice per $L$.

## A.4 Autovalori e autovettori

Un *autovettore* di un operatore lineare $L$ su uno spazio vettoriale $V$ é un vettore non nullo $|v\rangle \in V$ tale che $L|v\rangle = v|v\rangle$, dove $v$ é un numero complesso detto l'*autovalore* di $L$ corrispondente a $|v\rangle$. Gli autovalori di $L$ sono le soluzioni dell'equazione caratteristica $c(\lambda) = 0$, dove $c(\lambda) \equiv det|L - \lambda I|$, é il determinante della matrice $L - \lambda I$. L'*autospazio* corrispondente ad un autovalore $v$ é il sottospazio di $V$ formato da tutti i vettori che hanno autovalore $v$. Una *rappresenatzione diagonale* per un operatore $L$ é $L = \sum_i \lambda_i |i\rangle\langle i|$, dove i vettori $|i\rangle$ formano un insieme ortonormale di autovettori per $L$ con autovalori $\lambda_i$. Un operatore si dice diagonalizzabile se ammette una rappresentazione diaganale.

**Esercizio A.2** *Trovare autovettori, autovalori e rappresentazione diagonale delle matrici di Pauli*

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

## A.5 Operatori aggiunti e Hermitiani

Dato un operatore lineare $L$ su uno spazio di Hilbert $V$, esiste un unico operatore lineare $L^\dagger$ tale che per tutti i vettori $|v\rangle, |w\rangle \in V$,

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

L'operatore $L^\dagger$ si chiama l'aggiunto di $L$. Per convenzione, $|v\rangle^\dagger \equiv \langle v|$.

Dalla definizione seguono le seguenti proprietá:

- $(\sum_i a_i L_i)^\dagger = \sum_i a_i^* L_i^\dagger$.
- $(L^\dagger)^\dagger = L$.

In rappresentazione matriciale, l'operatore aggiunto corrisponde alla matrice trasposta coniugata di $L$: $L^\dagger = (L^*)^T$.

Un operatore *Hermitiano* é un operatore $L$ tale che $L^\dagger = L$.

Gli operatori di *proiezione* sono una classe importante di operatori Hermitiani, definiti nel seguente modo. Dato uno spazio vettoriale $V$ di dimensione $d$, si considera un sottospazio di $V$ di dimensione $k$. Allora, se $\{|1\rangle, \ldots, |d\rangle\}$ é una base ortonormale per $V$, il sottoinsieme $\{|1\rangle, \ldots, |k\rangle\}$ é una base ortonormale per $W$. Si definisce quindi

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i|$$

come la proiezione sul sottospazio $W$. Gli operatori di proiezione sono idempotenti: $P^2 = P$.

Un'altra classe importante di operatori lineari é quella degli operatori *normali*. $L$ é normale se e solo se $L^\dagger L = LL^\dagger$. Il teorema della *scomposizione spettrale* stabilisce che un operatore é normale se e solo se é *diagonalizzabile*, cioé puó essere scritto nella forma $M = \sum_i \lambda_i |i\rangle \langle i|$ dove $\lambda_i$ sono gli autovalori di $M$ e $\{|i\rangle\}$ forma una base ortonormale per $V$.

Una matrice Hermitiana é ovviamente normale. Si dimostra che una matrice Hermitiana é normale se e solo se ha autovalori reali.

Una matrice (o equivalentemente un operatore) $U$ si dice *unitaria* se $U^\dagger U = I$. Le matrici unitarie godono di un'importante proprietá, cioé preservano i prodotti interni. Infatti, se $U$ é unitaria, allora dati due vettori $|v\rangle$ e $|w\rangle$

$$(U|v\rangle, U|w\rangle) = \langle v| U^\dagger U |w\rangle = \langle v| I |w\rangle = \langle v, w\rangle.$$

Da questo risultato segue che la rappresentazione di un operatore unitario $U$ rispetto a due basi ortonormali di input e output $\{|v_i\rangle\}_i$ e $\{|w_i\rangle\}_i$ si puó dare in forma di prodotti esterni come:

$$U = \sum_i |w_i\rangle \langle v_i| .$$

**Esercizio A.3** *Mostrare che gli autovalori di una matrice unitaria hanno tutti modulo* 1 *e quindi possono essere scritti nella forma* $e^{i\theta}$ *con* $\theta \in \mathbb{R}$.

**Esercizio A.4** *Mostrare che le matrici di Pauli sono Hermitiane e unitarie.*